GUIDE TO OSCAL-BASED FEDRAMP SYSTEM SECURITY PLANS (SSP)

fedramp1.2.2-oscal1.0.x

August 12, 2022

FedRAMP

DOCUMENT REVISION HISTORY

Date	Description	Version	Author
11/27/2019	Initial Publication	1.0	FedRAMP PMO
1/24/2020	Adjusted citations to use OSCAL-provided "doc-id" instead of FedRAMP extension "ref-id"	1.1	FedRAMP PMO
8/1/2020	Aligned with OSCAL MR3 syntax. Aligned with new FedRAMP OSCAL Guides. Eliminated most required identifiers in favor of conformity tags. Revised approach to leveraged authorizations and customer responsibilities in controls.	2.0	FedRAMP PMO
2/10/2021	Aligned with OSCAL RC1 syntax. Eliminated conformity tags in favor of new core OSCAL syntax.	3.0	FedRAMP PMO
2/25/2021	Clarified revised registry approach and aligned with OSCAL RC2 syntax.	3.1	FedRAMP PMO
7/6/2021	Finalize alignment with OSCAL 1.0.0 syntax updates, update versioning scheme to match release strategy guidance.	fedramp1.0.0-oscal1.0.0	FedRAMP PMO
7/28/2021	Update table. Ensure guidance text in 5.4.1 aligns with code samples. Update this-system errata. Updates on inconsistent namespace and value usage. Update hyperlinks.	fedramp1.0.1-oscal1.0.0	FedRAMP PMO
8/10/2021	Fix control origination errors. Correct cloud-deployment-model and cloud-service-model documentation.	fedramp1.0.2-oscal1.0.0	FedRAMP PMO
8/12/2021	Review for updated release.	fedramp1.1.0-oscal1.0.0	FedRAMP PMO
8/28/2021	Fix errant interconnection field in 4.20.	fedramp1.1.1-oscal1.0.0	FedRAMP PMO
10/22/2021	Content improvements and review for minor and patch releases.	fedramp1.2.1-oscal1.0.0	FedRAMP PMO
8/12/2022	Content fixes and improvements.	Fedramp1.2.2-oscal1.0.x	FedRAMP PMO

How to Contact Us

For questions about FedRAMP, or for technical questions about this document including how to use it, contact *oscal@fedramp.gov.*

For more information about FedRAMP, see https://fedramp.gov.

TABLE OF CONTENTS

1. OVERVIEW

1.1. Who Should Use This Document?

This document is intended for technical staff and tool developers implementing solutions for importing, exporting, and manipulating Open Security Controls Assessment Language (OSCAL)-based FedRAMP System Security Plan (SSP) content.

It provides guidance and examples intended to guide an organization in the production and use of OSCAL-based FedRAMP-compliant SSP files. Our goal is to enable your organization to develop tools that will seamlessly ensure these standards are met so your security practitioners can focus on SSP content and accuracy rather than formatting and presentation.

1.2. Related Documents

This document does not stand alone. It provides information specific to developing tools to create and manage OSCAL-based, FedRAMP-compliant SSPs.

Refer to the *Guide to OSCAL-based FedRAMP Content* for foundational information and core concepts.

The *Guide to OSCAL-based FedRAMP Content*, contains foundational information and core concepts, which apply to all OSCAL-based FedRAMP guides. This document contains several references to that content guide.

1.3. Basic Terminology

XML and JSON use different terminology. Instead of repeatedly clarifying format-specific terminology, this document uses the following format-agnostic terminology through the document.

TERM	XML EQUIVALENT	JSON EQUIVALENT
`Field`	A single element or node that can hold a value or an attribute	A single object that can hold a value or property
`Flag`	Attribute	Property
`Assembly`	A collection of elements or nodes. Typically, a parent node with one or more child nodes.	A collection of objects. Typically, a parent object with one or more child objects.

These terms are used by National Institute of Standards and Technology (NIST) in the creation of OSCAL syntax.

Throughout this document, the following words are used to differentiate between requirements, recommendations, and options.

TERM	MEANING
must	Indicates a required action.
should	Indicates a recommended action, but not necessarily required.
may	Indicates an optional action.

2. FEDRAMP EXTENSIONS AND ALLOWED VALUES

NIST designed the core OSCAL syntax to model cybersecurity information that is common to most organization and compliance frameworks; however, NIST also recognized the need to provide flexibility or organizations with unique information needs.

A summary of the FedRAMP extensions and allowed values appears in the FedRAMP OSCAL Registry.

Instead of trying to provide a language that meets each organization's unique needs, NIST provided designed OSCAL with the ability to be extended.

As a result, FedRAMP-compliant OSCAL files are a combination of the core OSCAL syntax and extensions defined by FedRAMP. The *Guide to OSCAL-Based FedRAMP Content* describes the concepts behind FedRAMP extensions and allowed values. The extensions related to the System Security Plan (SSP) are cited in this document in context of their use.

These concepts are described in the Guide to OSCAL-based FedRAMP Content.

FedRAMP extensions and allowed values are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

Revised FedRAMP Registry Approach

The FedRAMP OSCAL Registry was originally provided as a spreadsheet. It now uses the draft OSCAL Extensions syntax and is offered in XML and JSON formats, with a human-readable HTML representation.

- *XML Version*
- *JSON Version*
- *HTML Version*

3. WORKING WITH OSCAL FILES

This section provides a summary of several important concepts and details that apply to OSCAL-based FedRAMP SSP files.

The *Guide to OSCAL-based FedRAMP Content* provides important concepts necessary for working with any OSCAL-based FedRAMP file. Familiarization with those concepts is important to understanding this guide.

3.1. XML and JSON Formats

The examples provided here are in XML; however, FedRAMP accepts XML or JSON formatted OSCAL-based SSP files. NIST offers a utility that provides lossless conversion of OSCAL-compliant files between XML and JSON in either direction.

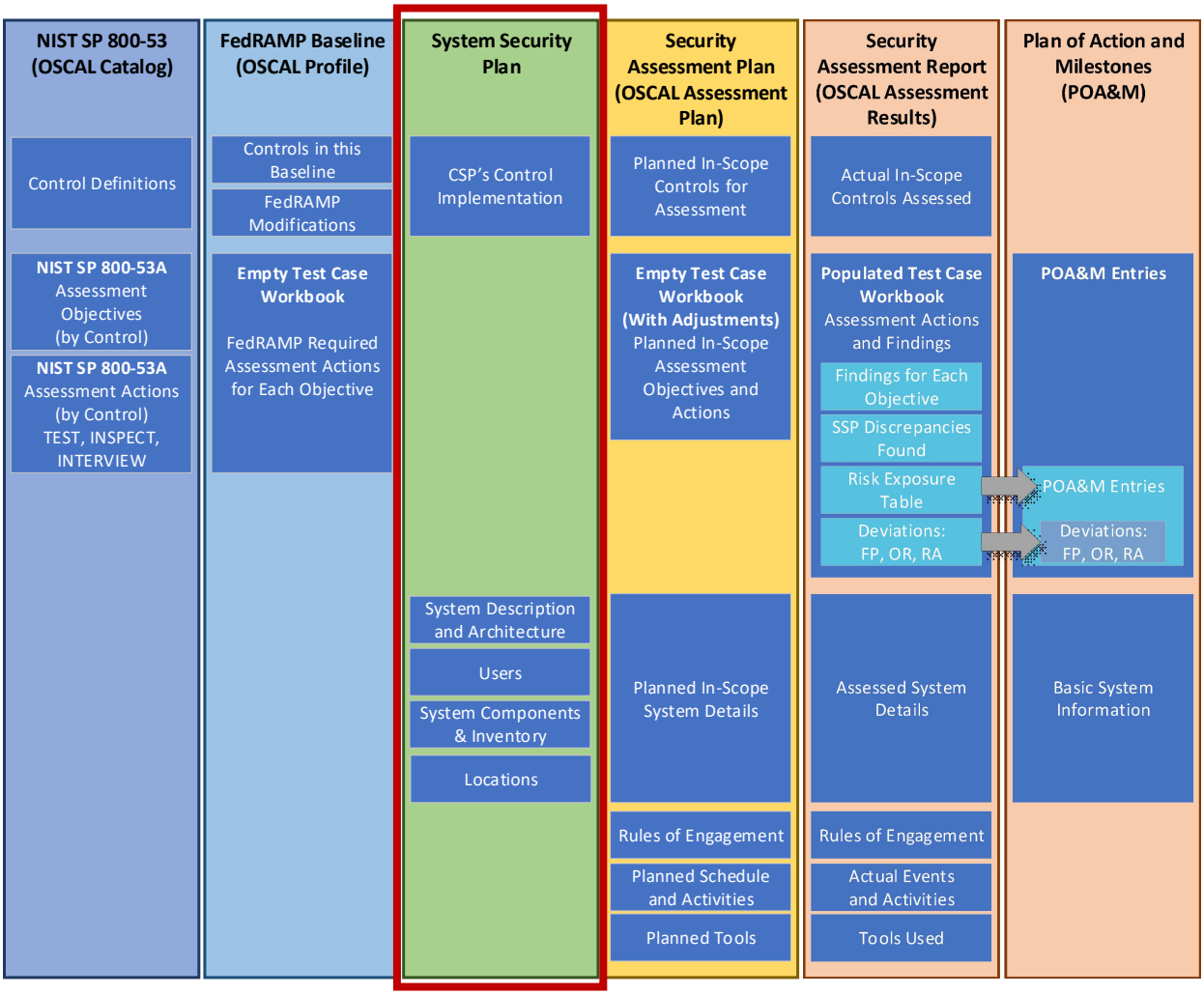
You may submit your SSP to FedRAMP using either format. If necessary, FedRAMP tools will convert the files for processing.

3.2. SSP File Concepts

Unlike the traditional MS Word-based SSP, SAP, and Security Assessment Report (SAR), the OSCAL-based versions of these files are designed to make information available through linkages, rather than duplicating information. In OSCAL, these linkages are established through `import` commands.

Each OSCAL file imports information from the one before it

For example, the NIST control definitions and FedRAMP baseline content that normally appears in Chapter 13 of the SSP are defined in the FedRAMP profile and simply referenced by the SSP.



Baseline Information is referenced instead of duplicated.

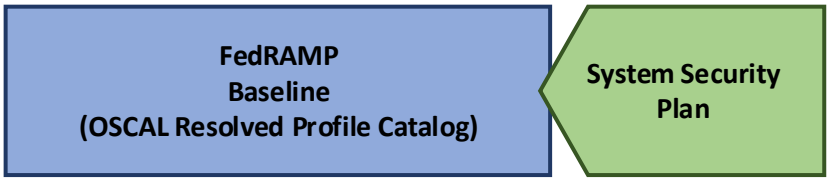
For this reason, an OSCAL-based SSP points to the appropriate OSCAL-based FedRAMP baseline as determined by the system's FIPS-199 impact level. Instead of duplicating control details, the OSCAL-based SSP simply points to the baseline content for information such as control definition statements, FedRAMP-added guidance, parameters, and FedRAMP-required parameter constraints.

3.2.1. Resolved Profile Catalogs

The resolved profile catalog for each FedRAMP baseline is a pre-processing of the profile and catalog to produce the resulting data. This reduces overhead for tools by eliminating the need to open and follow references from the profile to the catalog. It also includes only the catalog information relevant to the baseline, reducing the overhead of opening a larger catalog.

Where available, tool developers have the option of following the links from the profile to the catalog as described above, or using the resolved profile catalog.

Developers should be aware that at this time, catalogs and profiles remain relatively static. As OSCAL gains wider adoption, there is a risk that profiles and catalogs will become more dynamic, and a resolved profile catalog becomes more likely to be out of date. Early adopters may wish to start with the resolved profile catalog now, and plan to add functionality later for the separate profile and catalog handling later in their product roadmap.



The Resolved Profile Catalog for each FedRAMP Baseline reduces tool processing

For more information about resolved profile catalogs, see the *Guide to OSCAL-based FedRAMP Content Appendix C, Profile Resolution*.

3.3. OSCAL-based FedRAMP SSP Template

FedRAMP offers an OSCAL-based SSP shell file in both XML and JSON formats. This shell contains many of the FedRAMP required standards to help get you started. This document is intended to work in concert with that shell file. The OSCAL-based FedRAMP SSP Template is available in XML and JSON formats here:

- OSCAL-based FedRAMP SSP Template (JSON Format): https://github.com/GSA/fedramp-automation/raw/master/dist/content/templates/ssp/json/FedRAMP-SSP-OSCAL-Template.json
- OSCAL-based FedRAMP SSP Template (XML Format): https://github.com/GSA/fedramp-automation/raw/master/dist/content/templates/ssp/xml/FedRAMP-SSP-OSCAL-Template.xml

3.4. OSCAL's Minimum File Requirements

Every OSCAL-based FedRAMP SSP file must have a minimum set of required fields/assemblies, and must follow the OSCAL SSP core syntax found here:

https://pages.nist.gov/OSCAL/documentation/schema/implementation-layer/ssp

3.5. Importing the FedRAMP Baseline

OSCAL is designed for traceability. Because of this, the SSP is designed to be linked to the FedRAMP baseline. Rather than duplicating content from the baseline, the SSP is intended to reference the baseline content itself.

Use the `import-profile` field to specify an existing OSCAL-based SSP. The `href` flag may include any valid uniform resource identifier (URI), including a relative path, absolute path, or URI fragment.

SSP Import Representation

```
   <import-profile href="path/to/profile.xml" />

- OR -

   <import-profile href="#[uuid-value]" />
```

XPath Queries

```
(SSP) URI to Baseline:
  /*/import-profile/@href
```

If the value is a URI fragment, such as `#96445439-6ce1-4e22-beae-aa72cfe173d0`, the value to the right of the hashtag (#) is the UUID value of a resource in the SSP file's `back-matter`. Refer to the *Guide to OSCAL-based FedRAMP Content, Section 2.6, Citations, Attachments and Embedded Content in OSCAL Files*, for guidance on handling.

SSP Back Matter Representation

```
<back-matter>
    <resource uuid="96445439-6ce1-4e22-beae-aa72cfe173d0">
        <title>FedRAMP Moderate Baseline</title>
        <prop name="type" value="baseline" />
        <!-- Specify the XML or JSON file location. Only one required. -->
        <rlink media-type="application/xml" href="./CSP_System_SSP.xml" />
        <rlink media-type="application/json" href="./CSP_System_SSP.json" />
    </resource>
</back-matter>
```

XPath Queries

```
(SSP) Referenced OSCAL-based FedRAMP Baseline

XML:
  /*/back-matter/resource[@uuid='96445439-6ce1-4e22-beae-aa72cfe173d0']
  /rlink[@media-type='application/xml']/@href

OR JSON:
  /*/back-matter/resource[@uuid='96445439-6ce1-4e22-beae-aa72cfe173d0']
  /rlink[@media-type='application/json']/@href
```

Note: Cloud Service Providers must import FedRAMP profiles or resolved profile catalogs.

4. SSP TEMPLATE TO OSCAL MAPPING

For SSP-specific content, each page of the SSP is represented in this section, along with OSCAL code snippets for representing the information in OSCAL syntax. There is also XPath syntax for querying the code in an OSCAL-based FedRAMP SSP represented in XML format.

Content that is common across OSCAL file types is described in the *Guide to OSCAL-based FedRAMP Content*. This includes the following:

TOPIC	LOCATION
Title Page	*Guide to OSCAL-based FedRAMP Content, Section 4.1*
Prepared By/For	*Guide to OSCAL-based FedRAMP Content, Section 4.2 - 4.4*
Record of Template Changes	Not Applicable. Instead follow *Guide to OSCAL-based FedRAMP Content, Section 2.3.2, OSCAL Syntax Version*
Revision History	*Guide to OSCAL-based FedRAMP Content, Section 4.5*
How to Contact Us	*Guide to OSCAL-based FedRAMP Content, Section 4.6*
Document Approvers	*Guide to OSCAL-based FedRAMP Content, Section 4.7*
Acronyms and Glossary	*Guide to OSCAL-based FedRAMP Content, Section 4.8*
Laws, Regulations, Standards and Guidance	*Guide to OSCAL-based FedRAMP Content, Section 4.9*
Attachments and Citations	*Guide to OSCAL-based FedRAMP Content, Section 4.10*

It is not necessary to represent the following sections of the SSP template in OSCAL; however, tools should present users with this content where it is appropriate:

- Any blue-text instructions found in the SSP template, where the instructions are related to the content itself.
- Table of Contents
- Introductory and instructive content in sections 1 through 12, such as references to the NIST SP 800-60 Guide to Mapping Types, and the definitions from FIPS Pub 199.
- The control origination definitions are in Section 13 (Table 13-2); however, please note hybrid and shared are represented in OSCAL by specifying more than one control origination.

The OSCAL syntax in this guide may be used to represent the High, Moderate, and Low FedRAMP SSP Templates. Simply ensure the correct FedRAMP baseline is referenced using the `import-profile` statement.

The following pages are intended to be printed landscape on tabloid (11" x 17") paper.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

1. INFORMATION SYSTEM NAME/TITLE

This System Security Plan provides an overview of the security requirements for the Information System Name (Enter Information System Abbreviation) and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system. Information security is vital to our critical infrastructure and its effective performance and protection is a key component of our national security program. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the Enter Information System Abbreviation information system.

The security safeguards implemented for the Enter Information System Abbreviation system meet the policy and control requirements set forth in this System Security Plan. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

Table 1-1. Information System Name and Title

Unique Identifier	Information System Name	Information System Abbreviation
<Enter FedRAMP Application Number>	Information System Name	Enter Information System Abbreviation

4.1. Information System Name, Title, and FedRAMP Identifier

The FedRAMP-assigned application number is the unique ID for a FedRAMP system. OSCAL supports several system identifiers, which may be assigned by different organizations.

For this reason, OSCAL requires the `identifier-type` flag be present and have a value that uniquely identifies the issuing organization. FedRAMP requires its value to be "`https://fedramp.gov`" for all FedRAMP-issued application numbers.

Representation

```
<system-characteristics>
   <system-id identifier-type="https://fedramp.gov">F00000000</system-id>
   <system-name>System's Full Name</system-name>
   <system-name-short>System's Short Name or Acronym</system-name-short>
   <!-- description -->
</system-characteristics>
```

FedRAMP Allowed Value

Required Identifier Type:

- `identifier-type="https://fedramp.gov"`

XPath Queries

```
FedRAMP System Identifier:
  /*/system-characteristics/system-id[@identifier-type="https://fedramp.gov"]

Information System Name:
  /*/system-characteristics/system-name

Information System Abbreviation:
  /*/system-characteristics/system-name-short
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

2. INFORMATION SYSTEM CATEGORIZATION

The overall information system sensitivity categorization is recorded in Table 2-1. Security Categorization that follows. Directions for attaching the FIPS 199 document may be found in the following section: **Attachment 10. FIPS 199**.

Table 2-1. Security Categorization

System Sensitivity Level:	Choose level.

4.2. Information System Categorization and FedRAMP Baselines

Table 2-1 and Table 2-4 Representation

```
<system-characteristics>
    <!-- description -->
    <prop name="authorization-type" ns="https://fedramp.gov/ns/oscal"
          value="fedramp-agency"/>
    <!-- prop, link, date-authorized -->
    <security-sensitivity-level>fips-199-moderate</security-sensitivity-level>
    <!-- system-information -->
</system-characteristics>
```

FedRAMP Extensions & Allowed Values

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="authorization-type"`
  - **Valid:** `fedramp-jab, fedramp-agency, fedramp-li-saas`

OSCAL Allowed Values

Valid values for `security-sensitivity-level`:

- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

XPath Queries

```
System Sensitivity Level:
  /*/system-characteristics/security-sensitivity-level

URL to OSCAL-based FedRAMP Baseline File:
  /*/import-profile/@href

FedRAMP Authorization Type:
  /*/system-characteristics/prop[@name="authorization-type"]
  [@ns="https://fedramp.gov/ns/oscal"]
```

NOTES:

- The identified System Sensitivity Level governs which FedRAMP baseline applies. See Appendix A for more information about importing the appropriate FedRAMP baseline.

The `adjustment-justification` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP Alowed Values

FedRAMP only accepts NIST SP 800-60 IDs. The `system` flag of the `information-type-id` field must be:

- `https://doi.org/10.6028/NIST.SP.800-60v2r1`

NIST Allowed Values

Valid impact (base/selected) values:

- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availabili
System Development	C.3.5.1	Low	Moderate	Low

Table 2-2. Sensitivity Categorization of Information Types

Information Type (Use only information types from NIST SP 800-60, Volumes I and II as amended)	NIST 800-60 identifier for Associated Information Type	Confidentiality	Integrity	Availability
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.
<Enter Information Type>	<Enter NIST Identifier>	Choose level.	Choose level.	Choose level.

4.3. Information Types

Table 2-2 and Table 15-9 Representation

```
<system-information>
    <!-- security-sensitivity-level -->
    <information-type uuid="uuid-of-information-type">
        <title>Information Type Name</title>
        <categorization system="https://doi.org/10.6028/NIST.SP.800-60v2r1">
            <information-type-id>C.2.4.1</information-type-id>
        </categorization>
        <confidentiality-impact>
            <base>fips-199-moderate</base>
            <selected>fips-199-moderate</selected>
            <adjustment-justification><p>Description</p></adjustment-justification>
        </confidentiality-impact>
        <integrity-impact>
            <base>fips-199-moderate</base>
            <selected>fips-199-moderate</selected>
            <adjustment-justification><p>Description</p></adjustment-justification>
        </integrity-impact>
        <availability-impact>
            <base>fips-199-moderate</base>
            <selected>fips-199-moderate</selected>
            <adjustment-justification><p>Description</p></adjustment-justification>
        </availability-impact>
    </information-type>
    <!-- repeat the information-type assembly for each information type -->
    <!-- security-impact-levels -->
</system-information>
```

NOTES:

- Table 2-2 is a subset of Table 15-9. The above OSCAL representation satisfies both.
- For each impact type, if the `selected` field does not match the `base` field, the `adjustment-justification` field is required.

Table 2-2 is a sub-set of Table 15-9 as follows:

Table Column	Table 2-2	Table 15-9	XPath Queries
Information Type	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/title`
NIST 800-60 Identifier	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/information-type-id [@system="https://doi.org/10.6028/NIST.SP.800-60v2r1"]`
NIST Recommended Confidentiality Impact Level	No	**Yes**	`//system-characteristics/system-information/information-type[1]/confidentiality-impact/base`
NIST Recommended Integrity Impact Level	No	**Yes**	`//system-characteristics/system-information/information-type[1]/integrity-impact/base`
NIST Recommended Availability Impact Level	No	**Yes**	`//system-characteristics/system-information/information-type[1]/availability-impact/base`
CSP Selected Confidentiality Impact Level	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/confidentiality-impact/selected`
CSP Selected Integrity Impact Level	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/integrity-impact/selected`
CSP Selected Availability Impact Level	**Yes**	**Yes**	`//system-characteristics/system-information/information-type[1]/availability-impact/selected`
Impact Adjustment Justification	No	**Yes**	`//system-characteristics/system-information/information-type[1]/confidentiality-impact/adjustment-justification` `//system-characteristics/system-information/information-type[1]/integrity-impact/adjustment-justification` `//system-characteristics/system-information/information-type[1]/availability-impact/adjustment-justification`

In each XPath query in the table above, replace the "[1]" with "[2]", "[3]"", as needed, up to the number of information-type fields that exist in the file.

Use the following XPath statement to count the number of information-type fields: `count(//system-characteristics/system-information/information-type)`

The FedRAMP SSP Template has only one place to provide the justification of changing any of the three recommended NIST 800-60 levels. OSCAL ties this justification to its individual type (confidentiality, availability, or integrity). If recreating Table 15-9 from OSCAL data, display all three justifications in this single field, and label each.

2.2. Security Objectives Categorization (FIPS 199)

Based on the information provided in Table 2-2. Sensitivity Categorization of Information Types, for the Enter Information System Abbreviation, default to the high-water mark for the Information Types as identified in Table 2-3. Security Impact Level below.

Table 2-3. Security Impact Level

Security Objective	Low, Moderate or High
Confidentiality	Choose level.
Integrity	Choose level.
Availability	Choose level.

Through review and analysis, it has been determined that the baseline security categorization for the Enter Information System Abbreviation system is listed in the Table 2-4. Baseline Security Configuration that follows.

Table 2-4. Baseline Security Configuration

Enter Information System Abbreviation Security Categorization	Choose level

Using this categorization, in conjunction with the risk assessment and any unique security requirements, we have established the security controls for this system, as detailed in this SSP.

4.4. Security Objectives Categorization (FIPS 199)

Representation

```
<system-characteristics>
    <!-- cut -->
    <security-sensitivity-level>moderate</security-sensitivity-level>
    <!-- system-information -->




    <security-impact-level>
        <security-objective-confidentiality>fips-199-moderate
        </security-objective-confidentiality>

        <security-objective-integrity>fips-199-moderate</security-objective-integrity>
        <security-objective-availability>fips-199-moderate

        </security-objective-availability>
    </security-impact-level>
    <!-- status -->
</system-characteristics>
```

NIST Allowed Values
Valid security sensitivity values:
- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

NIST Allowed Values
Valid security objective values:
- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

XPath Queries

```
System Sensitivity Level:
  /*/system-characteristics/security-sensitivity-level


Security Objective: Confidentiality:
  /*/system-characteristics/security-impact-level/security-objective-confidentiality
Security Objective: Integrity:
  /*/system-characteristics/security-impact-level/security-objective-integrity
Security Objective: Availability:
  /*/system-characteristics/security-impact-level/security-objective-availability
```

NOTES:

- The `security-sensitivity-level` field in the OSCAL file satisfies both Table 2-1 and 2-4.

2.3. Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels corresponding to each function being performed.

The digital identity level is Choose an item.

4.5. Digital Identity Determination

The digital identity level identified in Section 2.3 is the same as the level in Attachment 3. Both are identified with the same single piece of information. This is an aggregate of the individual IAL, AAL, and FAL designations which are required in the digital identity worksheet.

Representation

```
<system-characteristics>

    <!-- Attachment 3, Digital Identity Worksheet (required by FedRAMP) -->
    <prop name="identity-assurance-level" value="1"/>
    <prop name="authenticator-assurance-level" value="1"/>
    <prop name="federation-assurance-level" value="1"/>

</system-characteristics>
```

NIST Allowed Values
Valid IAL, AAL, and FAL values (as defined by NIST 800-63):

- 1
- 2
- 3

XPath Queries

```
Identity Assurance Level:
  /*/system-characteristics/prop[@name="identity-assurance-level"]/@value

Authenticator Assurance Level:
  /*/system-characteristics/prop[@name="authenticator-assurance-level"]/@value

Federation Assurance Level:
  /*/system-characteristics/prop[@name="federation-assurance-level"]/@value
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

3. INFORMATION SYSTEM OWNER

The following individual is identified as the system owner or functional proponent/advocate for this system.

Table 3-1. Information System Owner

Information System Owner Information	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

NOTES ON ADDRESSES

Preferred Approach: When multiple parties share the same address, such as multiple staff members at a company HQ, define the location once as a `location` assembly, then use the `location-uuid` field within each `party` assembly to identify the location of that individual or team.

Alternate Approach: If the address is unique to this individual, it may be included in the `party` assembly itself.

Hybrid Approach: It is possible to include both a `location-uuid` and an `address` assembly within a `party` assembly. This may be used where multiple staff are in the same building, yet have different office numbers or mail stops. Use the `location-uuid` to identify the shared building, and only include a single `addr-line` field within the party's `address` assembly.

A tool developer may elect to always create a location assembly, even when only used once; however, tools must recognize and handle all of the approaches above when processing OSCAL files.

4.6. Information System Owner

A role with an ID value of "`system-owner`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the System Owner's information.

Representation

```
<metadata>
    <!-- cut -->
    <role id="system-owner"><!-- cut --></role>
    <location uuid="uuid-of-hq-location">
        <title>CSP HQ</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-1" type="person">
        <name>[SAMPLE]Person Name 1</name>
        <prop name="job-title" value="Individual's Title"/>
            <prop name="mail-stop" value="A-1"/>
                <email-address>name@example.com</email-address>
                <telephone-number>202-000-0000</telephone-number>
                <location-uuid>uuid-of-hq-location</location-uuid>
                <member-of-organization>uuid-of-csp</member-of-organization>
    </party>
    <responsible-party role-id="system-owner">
        <party-uuid>uuid-of-person-1</party-uuid>
    </responsible-party>
</metadata>
```

NIST Allowed Value

Required role ID:

- `system-owner`

XPath Queries

```
System Owner's Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-owner"]/
  party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

System Owner's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="system-owner"]/party-uuid]]/location-uuid]/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

System Owner's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-owner"]/
  party-uuid]]/prop[@name='job-title']/@value

Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="system-owner"]/party-uuid]]/member-of-organization]/name
```

NOTE:

- If no country is provided, FedRAMP tools will assume a US address.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

4. AUTHORIZING OFFICIALS

Instruction: The Authorizing Official is determined by the authorization.

JAB P-ATO: FedRAMP, JAB, as comprised of member rep Administration (GSA), Department of Defense (DoD) and

Agency Authority to Operate (ATO): Agency Authorizing

Delete this and all other instructions from your final ver

The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the *Insert AO information as instructed above.*

FedRAMP Extension:

prop (`ns="https://fedramp.gov/ns/oscal"`)

- `name="authorization-type"`

FedRAMP Allowed Values

- `fedramp-jab`
- `fedramp-agency`
- `fedramp-li-saas`

FedRAMP JAB P-ATO Authorization Representation

NIST Allowed Value

Required Role ID:

- `authorizing-official`

```
<metadata>
    <!-- cut -->
    <role id="authorizing-official">
        <title>Authorizing Official</title>
        <desc>The government executive(s) who authorize this system.</desc>
    </role>
    <!-- cut -->
    <party uuid="uuid-of-fedramp-jab" type="organization">
        <name>FedRAMP: Joint Authorization Board</name>
        <short-name>FedRAMP JAB</short-name>
    </party>
    <!-- cut -->
    <responsible-party role-id="authorizing-official">
        <party-uuid>uuid-of-fedramp-jab</party-uuid>
    </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
    <!-- description -->
    <prop name="authorization-type"
          ns="https://fedramp.gov/ns/oscal">fedramp-jab</prop>
    <!-- prop -->
</system-characteristics>
```

JAB XPath Queries

```
Authorizing Official's Name:
  //metadata/party[@uuid=[//metadata/responsible-party[@role-id="authorizing-
  official"]/party-uuid]]/name
```

Controlled Unclassified Information

4.7. Authorizing Officials

A role with an ID value of "`authorizing-official`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the Authorizing Official's information.

FedRAMP Agency Authorization Representation

```
<metadata>
    <role id="authorizing-official">
        <title>Authorizing Official</title>
    </role>
    <party uuid="uuid-of-agency" type="organization">
        <name>Agency Name</name>
    </party>
    <party uuid="uuid-of-person-6" type="person">
        <name>[SAMPLE]Person Name 6</name>
        <prop name="job-title" value="Individual's Title"/>
            <email-address>name@example.com</email-address>
            <telephone-number>202-000-0000</telephone-number>
            <member-of-organization>uuid-of-agency</member-of-organization>
    </party>
    <responsible-party role-id="authorizing-official">
        <party-uuid>uuid-of-person-6</party-uuid>
    </responsible-party>
</metadata>
<!-- import -->
<system-characteristics>
    <!-- description -->
    <prop name="authorization-type"
          ns="https://fedramp.gov/ns/oscal"
          value="fedramp-agency" />
    <!-- prop -->
</system-characteristics>
```

Authorization Type XPath Query

```
FedRAMP Authorization Type:
  /*/system-characteristics/prop[@name="authorization-type"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value
```

FedRAMP Agency and LI-SaaS XPath Queries

```
Authorizing Official's Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="authorizing-official"]/party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

Authorizing Official's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="authorizing-official"]/party-uuid]]/prop[@name='job-title']

Authorizing Official's Agency:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="authorizing-official"]/party-uuid]]/member-of-organization]/name
```

NOTE:

- If the `authorization-type` field is "`fedramp-jab`", the `responsible-party/party-uuid` field must be the uuid value for the FedRAMP JAB.

5. OTHER DESIGNATED CONTACTS

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

Delete this and all other instructions from your final version of this document.

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5-1. Information System Management Point of Contact

Information System Management Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 5-2. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Next Page

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

Point of Contact	
Name	<Enter Name>
Title	<Enter Title>

4.8. Other Designated Contacts: Information System Management

A role with an ID value of "`system-poc-management`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the Information System Manager's information.

Table 5-1 Representation

NIST Allowed Value
Required Role IDs:
- `system-poc-management`

```
<metadata>
    <!-- cut -->
    <role id="system-poc-management"><!-- cut --></role>
    <location uuid="uuid-of-hq-location">
        <title>CSP HQ</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-5" type="person">
        <name>[SAMPLE]Person Name 5</name>
        <prop name="job-title" value="Individual's Title" />
            <email-address>name@org.domain</email-address>
            <telephone-number>202-000-0000</telephone-number>
            <location-uuid>uuid-of-hq-location</location-uuid>
            <member-of-organization>uuid-of-csp</member-of-organization>
    </party>
    <responsible-party role-id="system-poc-management">
        <party-uuid>uuid-of-person-5</party-uuid>
    </responsible-party>
</metadata>
```

XPath Queries

```
Information System Management POC Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-poc-management"]/
  party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

Information System Management POC's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="system-poc-management"]/party-uuid]]/location-uuid]/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

Information System Management POC's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-poc-management"]/
  party-uuid]]/prop[@name='job-title']

Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-
  party[@role-id="system-poc-management"]/party-uuid]]/member-of-
  organization]/name
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

5. OTHER DESIGNATED CONTACTS

Instruction: AOs should use the following section to identify points of contact that understand the technical implementations of the identified cloud system. AOs should edit, add, or modify the contacts in this section as they see fit.

Delete this and all other instructions from your final version of this document.

The following individual(s) identified below possess in-depth knowledge of this system and/or its functions and operation.

Table 5-1. Information System Management Point of Contact

Information System Management Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

See Previous Page

Table 5-2. Information System Technical Point of Contact

Information System Technical Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Instruction: Add more tables as needed.

Delete this and all other instructions from your final version of this document.

Point of Contact	
Name	<Enter Name>
Title	<Enter Title>

4.9. Other Designated Contacts: Information System Technical

Role assemblies with ID values of "`system-poc-technical`" and "`system-poc-other`" are required. Use `responsible-party` assemblies to associate these roles with the party assemblies containing the system points of contact.

Table 5-2 Representation

NIST Allowed Values

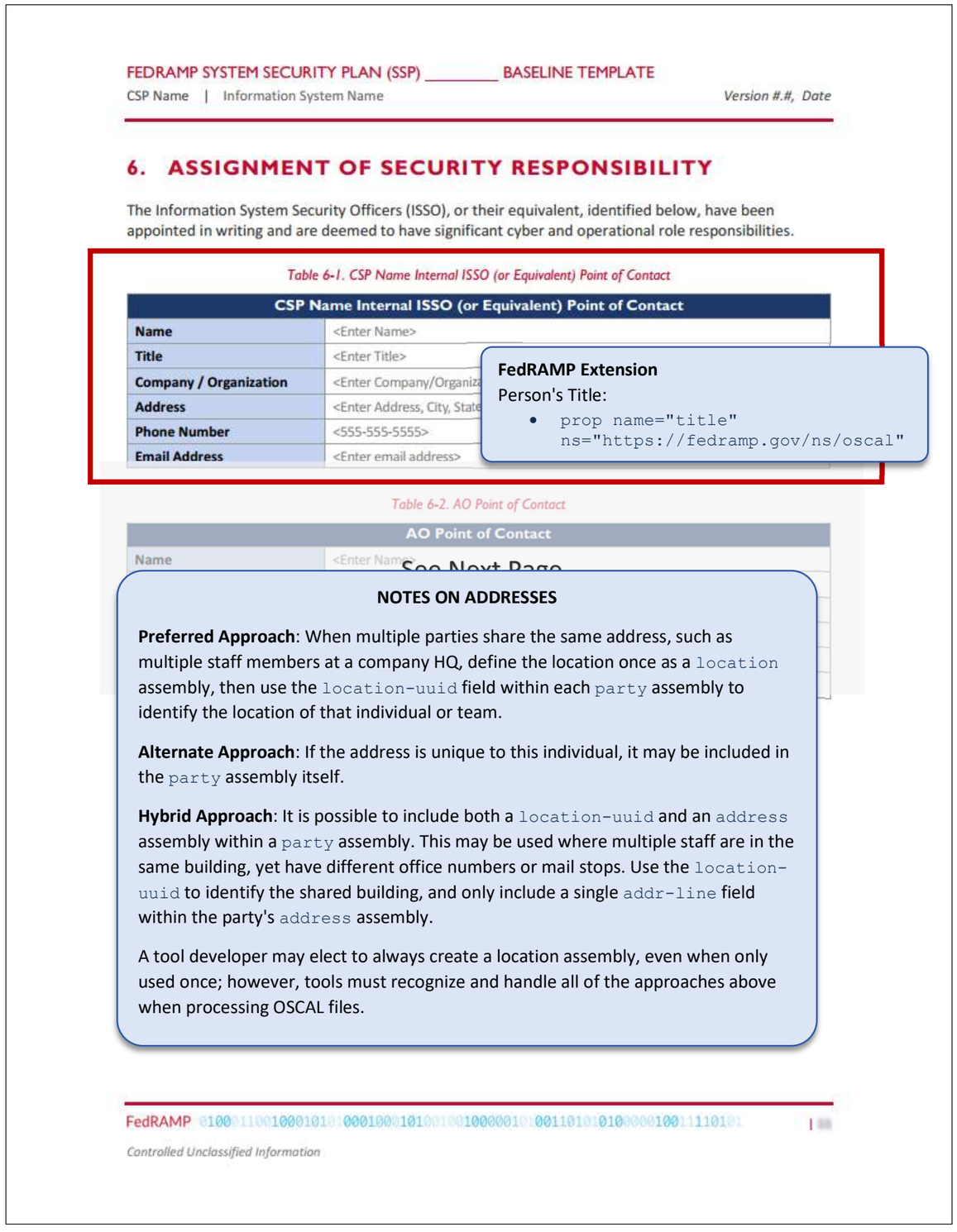
Required Role IDs:

- `system-poc-technical`
- `system-poc-other`

```
<metadata>
    <!-- cut -->
    <role id="system-poc-technical"><!-- cut --></role>
    <role id="system-poc-other"><!-- cut --></role>
    <location uuid="uuid-of-hq-location">
        <title>CSP HQ</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-7" type="person">
        <name>[SAMPLE]Person Name 7</name>
        <prop name="job-title" value="Individual's Title"/>
        <email-address>name@org.domain</email-address>
        <telephone-number>202-000-0000</telephone-number>
        <location-uuid>uuid-of-hq-location</location-uuid>
        <member-of-organization>uuid-of-csp</member-of-organization>
    </party>
    <!-- repeat party assembly for each person -->
    <responsible-party role-id="system-poc-technical">
        <party-uuid>uuid-of-person-7</party-uuid>
    </responsible-party>
    <responsible-party role-id="system-poc-other">
        <party-uuid>uuid-of-person-8</party-uuid>
        <party-uuid>uuid-of-person-9</party-uuid>
    </responsible-party>
</metadata>
```

XPath Queries

```
Information System Technical POC Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-poc-technical"]/
  party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

Information System Technical POC's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="system-poc-technical"]/party-uuid]]/location-uuid]/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

Information System Technical POC's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="system-poc-technical"]/
  party-uuid]]/prop[@name='job-title']

Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-
  party[@role-id="system-poc-technical"]/party-uuid]]/member-of-
  organization]/name
```



FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Company / Organization	<Enter Company/Organiz
Address	<Enter Address, City, State
Phone Number	<555-555-5555>
Email Address	<Enter email address>

FedRAMP Extension

Person's Title:

- `prop name="title" ns="https://fedramp.gov/ns/oscal"`

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>

See Next Page

NOTES ON ADDRESSES

Preferred Approach: When multiple parties share the same address, such as multiple staff members at a company HQ, define the location once as a `location` assembly, then use the `location-uuid` field within each `party` assembly to identify the location of that individual or team.

Alternate Approach: If the address is unique to this individual, it may be included in the `party` assembly itself.

Hybrid Approach: It is possible to include both a `location-uuid` and an `address` assembly within a `party` assembly. This may be used where multiple staff are in the same building, yet have different office numbers or mail stops. Use the `location-uuid` to identify the shared building, and only include a single `addr-line` field within the party's `address` assembly.

A tool developer may elect to always create a location assembly, even when only used once; however, tools must recognize and handle all of the approaches above when processing OSCAL files.

4.10. Assignment of Security Responsibility: Information System Security Officer (ISSO)

A role with an ID value of "`information-system-security-officer`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the Information System Security Officer's information.

Table 6-1 Representation

```
<metadata>
    <!-- cut -->
    <role id="information-system-security-officer"><!-- cut -->
        <title>System Information System Security Officer (or Equivalent)</title>
    </role>
    <location uuid="uuid-of-hq-location">
        <title>CSP HQ</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Haven</city>
            <state>ME</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-10" type="person">
        <name>[SAMPLE]Person Name 10</name>
        <prop name="job-title" value="Individual's Title"/>
        <email-address>name@org.domain</email-address>
        <telephone-number>202-000-0000</telephone-number>
        <location-uuid>uuid-of-hq-location</location-uuid>
        <member-of-organization>uuid-of-csp</member-of-organization>
    </party>
    <!-- repeat party assembly for each person -->
    <responsible-party role-id="system-poc-technical">
        <party-uuid>uuid-of-person-7</party-uuid>
    </responsible-party>
</metadata>
```

NIST Allowed Value

Required Role ID:

- `information-system-security-officer`

XPath Queries

```
ISSO POC Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="information-system-
  security-officer"]/party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

ISSO POC's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="information-system-security-officer"]/party-uuid]]/location-uuid]/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

ISSO POC's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="information-system-
  security-officer"]/party-uuid]]/prop[@name='job-title']

Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party
  [@role-id="information-system-security-officer"]/party-uuid]]/member-of-
  organization]/name
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

6. ASSIGNMENT OF SECURITY RESPONSIBILITY

The Information System Security Officers (ISSO), or their equivalent, identified below, have been appointed in writing and are deemed to have significant cyber and operational role responsibilities.

Table 6-1. CSP Name Internal ISSO (or Equivalent) Point of Contact

CSP Name Internal ISSO (or Equivalent) Point of Contact	
Name	<Enter See Previous Page
Title	<Enter Title>
Company / Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

Table 6-2. AO Point of Contact

AO Point of Contact	
Name	<Enter Name>
Title	<Enter Title>
Organization	<Enter Company/Organization>.
Address	<Enter Address, City, State and Zip>
Phone Number	<555-555-5555>
Email Address	<Enter email address>

4.11. Assignment of Security Responsibility: Authorizing Official (AO) POC

A role with an ID value of "`authorizing-official-poc`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the Authorizing Official's information.

Table 6-2 Representation

```
<metadata>
    <!-- cut -->
    <role id="authorizing-official-poc">
        <title>Authorizing Official's Point of Contact</title>
    </role>
    <location uuid="uuid-of-agency-office">
        <title>Agency Office</title>
        <address type="work">
            <addr-line>1234 Some Street</addr-line>
            <city>Washington</city>
            <state>DC</state>
            <postal-code>00000</postal-code>
        </address>
    </location>
    <party uuid="uuid-of-agency" type="organization">
        <name>Full Agency Name Here</name>
        <short-name>FANH</short-name>
    </party>
    <party uuid="uuid-of-person-11" type="person">
        <name>[SAMPLE]Person Name 11</name>
        <prop name="job-title" value="Individual's Title"/>
        <email-address>name@org.domain</email-address>
        <telephone-number>202-000-0000</telephone-number>
        <location-uuid>uuid-of-agency-office</location-uuid>
        <member-of-organization>uuid-of-agency</member-of-organization>
    </party>
    <!-- repeat party assembly for each person -->
    <responsible-party role-id="authorizing-official-poc">
        <party-uuid>uuid-of-person-11</party-uuid>
    </responsible-party>
</metadata>
```

NIST Allowed Value

Required Role ID:

- `authorizing-official-poc`

XPath Queries

```
AO POC Name:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="authorizing-official-poc"]/
  party-uuid]]/name

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

AO POC's Address:
  /*/metadata/location[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party [@role-
  id="authorizing-official-poc"]/party-uuid]]/location-uuid]/address/addr-line

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

AO POC's Title:
  /*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="authorizing-official-poc"]/
  party-uuid]]/prop[@name='job-title']

Company/Organization:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-
  party[@role-id="authorizing-official-poc"]/party-uuid]]/member-of-
  organization]/name
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

7. INFORMATION SYSTEM OPERATIONAL STATUS

The system is currently in the life-cycle phase shown in Table 7-1. System Status that follows. (Only operational systems can be granted an ATO).

Table 7-1. System Status

System Status		
☐	Operational	The system is operating and in production.
☐	Under Development	The system is being designed, developed, or implemented
☐	Major Modification	The system is undergoing a major change, development, or transition.
☐	Other	Explain: Click here to enter text.

Instruction: Select as many status indicators as apply. If more than one status is selected, list which components of the system are covered under each status indicator.

Delete this and all other instructions from your final version of this document.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

4.12. Information System Operational Status

Representation

```
<system-characteristics>
    <!-- cut -->

    <!-- security-impact-level -->
    <status state="operational">
        <remarks>
            <p>Remarks are optional if status/state is "operational".</p>
            <p>Remarks are required otherwise.</p>
        </remarks>
    </status>
    <!-- leveraged-authorization -->




    <!-- cut -->
</system-characteristics>
```

NIST Allowed Values

FedRAMP only accepts those in bold:

- **`operational`**
- `under-development`
- **`under-major-modification`**
- `disposition`
- **`other`**

XPath Queries

```
System's Operational Status:
  /*/system-characteristics/status/@state

Remarks on System's Operational Status:
  /*/system-characteristics/status/remarks/node()
```

NOTE:

- If the status is "`other`", the `remarks` field is required. Otherwise it is optional.
- While `under-development`, and `disposition` are valid OSCAL values, systems with either of these operational status values are not eligible for a FedRAMP Authorization.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1. Service Layers Represented in this SSP that follows.

Instruction: Check all layers that apply.

Delete this and all other instructions from your final version of this document.

Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
☐	Software as a Service (SaaS)	Major Application
☐	Platform as a Service (PaaS)	Major Application
☐	Infrastructure as a Service (IaaS)	General Support System
☐	Other	**Explain:** Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

4.13. Cloud Service Models

Representation

```
<system-characteristics>
    <!-- cut -->



    <!-- prop -->
    <prop name="cloud-service-model" value="saas">
        <remarks>
            <p>Remarks are required if service model is "other". Optional otherwise.</p>
        </remarks>
    </prop>
    <!-- link or date authorized -->




    <!-- cut -->
</system-characteristics>
```

NIST Allowed Values

Valid Service Model values:

- `saas`
- `paas`
- `iaas`
- `other`

XPath Queries

```
Service Model:
  /*/system-characteristics/prop[@name="cloud-service-model"]/@value

Remarks on System's Service Model:
  /*/system-characteristics/prop[@name="cloud-service-model"]/remarks/node()
```

NOTE:

- A cloud service provider may define two or more cloud service models for the cloud service offering defined in the system security plan if applicable for customer use (IaaS and PaaS; IaaS and PaaS and SaaS; PaaS and SaaS). Cloud service providers may use a "`cloud-service-model`" `prop` for each applicable cloud service model.
- If the service model is "`other`", the `remarks` field is required. Otherwise it is optional.

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2. Cloud Deployment Model Represented in this SSP that follows.

Instruction: Check deployment model that applies.

Delete this and all other instructions from your final version of this document.

Table 8-2. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
☐	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
☐	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
☐	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
☐	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

FedRAMP Extensions and Accepted Values

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="cloud-deployment-model"`
  Valid: `public-cloud, private-cloud, government-only-cloud, hybrid-cloud, other`

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

ss

4.14. Cloud Deployment Models

Representation

```
<system-characteristics>
    <!-- cut -->



    <!-- prop -->
    <prop name="cloud-deployment-model" value="public-cloud">
        <remarks>
            <p>Remarks are required if deployment model is "hybrid". Optional otherwise.</p>
        </remarks>
    </prop>
    <!-- link or date authorized -->



    <!-- cut -->
</system-characteristics>
```

XPath Queries

```
Deployment Model:
  /*/system-characteristics/prop[@name="cloud-deployment-model"]/@value

Remarks on System's Deployment Model:
  /*/system-characteristics/prop[@name="cloud-deployment-model"]/remarks/node()
```

NOTE:

- A cloud service provider may define one and only one cloud deployment model in the system security plan for a cloud service offering.
- OSCAL 1.0.0 permits `a cloud-deployment-model` of value `community-cloud`, but FedRAMP does not permit such a deployment model for cloud service offerings and is not permitted for a FedRAMP OSCAL-based system security plan.
- If the deployment model is "`hybrid`", the `remarks` field is required. Otherwise it is optional.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

8.3. Leveraged Authorizations

Instruction: The FedRAMP program qualifies different service layers for Authorizations. One or multiple service layers can be qualified in one System Security Plan. If a lower level layer has been granted an Authorization and another higher level layer represented by this SSP plans to leverage a lower layer's Authorization, this System Security Plan must clearly state that intention. If an information system does not leverage any pre-existing Authorizations, write "None" in the first column of the table that follows. cAdd as many rows as necessary in the table that follows.

Delete this and all other instructions from your final version of this document.

The Enter Information System Abbreviation Choose an item leverages a pre-existing FedRAMP Authorization. FedRAMP Authorizations leveraged by this Enter Information System Abbreviation are listed in Table 8-3. Leveraged Authorizations that follows.

Table 8-3. Leveraged Authorizations

Leveraged Information System Name	Leveraged Service Provider Owner	Date Granted
<Enter Leveraged information system name1>	<Enter service provider owner1>	<Date>
<Enter Leveraged information system name2>	<Enter service provider owner2>	<Date>
<Enter Leveraged information system name3>	<Enter service provider owner3>	<Date>

IMPORTANT FOR LEVERAGED SYSTEMS:

While a leveraged system has no need to represent content here, its SSP must include special inheritance and responsibility information in the individual controls. See *Section 5.4.8, Response: Identifying Inheritable Controls and Customer Responsibilities* for more information.

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

The `authorization-date` field is string type *date*, which requires a four digit year, a dash, a two digit month, a dash, a two digit day, and an optional timezone offset. (`yyyy-mm-dd` or `yyyy-mm-dd-05:00`)

For more information, visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#date

Additional information is required within each control. See *Section 5.4.9, Leveraged Authorization Response: Inheriting Controls, Satisfying Responsibilities* for more information.

4.15. Leveraged Authorizations

If this system is leveraging the authorization of one or more systems, such as a SaaS running on an IaaS, each leveraged system must be represented within the `system-implementation` assembly. There must be one `leveraged-authorization` assembly and one matching `component` assembly for each leveraged authorization.

The `leveraged-authorization` assembly includes the leveraged system's name, POC, and authorization date. The `component` assembly must be linked to the `leveraged-authorization` assembly using a property (`prop`) field with the name `leveraged-authorization-uuid` and the UUID value of its associated `leveraged-authorization` assembly. The `component` assembly enables controls to reference it with the `by-component` responses described in *Section 5.4, Control Implementation Descriptions*. The `implementation-point` property value must be set to "`external`".

If the leveraged system owner provides a UUID for their system, such as in an OSCAL-based Inheritance and Responsibility document (similar to a CRM), it should be provided as the `inherited-uuid` property value.

Representation

```
<metadata>
    <party uuid="uuid-value">
        <name>Example IaaS Provider</name>
        <short-name>E.I.P.</short-name>
    </party>
</metadata>
<!-- import-profile, system-characteristics -->
<system-implementation>
    <!-- prop -->
    <leveraged-authorization uuid="uuid-value" >
        <title>Name of Underlying System</title>
        <prop name="leveraged-system-identifier"
            ns="https://fedramp.gov/ns/oscal"
            value="Package_ID value" />
        <link href="//path/to/leveraged_system_legacy_crm.xslt" />
        <link href="//path/to/leveraged_system_responsibility_and_inheritance.xml" />
        <party-uuid>uuid-of-leveraged-system-poc</party-uuid>
        <date-authorized>2015-01-01</date-authorized>
    </leveraged-authorization>
    <!-- user -->
    <component uuid="uuid-of-leveraged-system" type="leveraged-system">
        <title>Name of Leveraged System</title>
        <description>
            <p>Briefly describe leveraged system.</p>
        </description>
        <prop name="leveraged-authorization-uuid"
            value="5a9c98ab-8e5e-433d-a7bd-515c07cd1497" />
            <prop name="inherited-uuid" value="11111111-0000-4000-9001-000000000001" />
                <prop name="implementation-point" value="external"/>
                <status state="operational"/>
    </component>
</system-implementation>
```

The `title` field must match an existing FedRAMP authorized Cloud_Service_Provider_Package property value.

A `leveraged-system-identifier` property must be provided within each `leveraged-authorization` field.. The value of this property must be from the same Cloud Service Provider as identified in the `title` field.

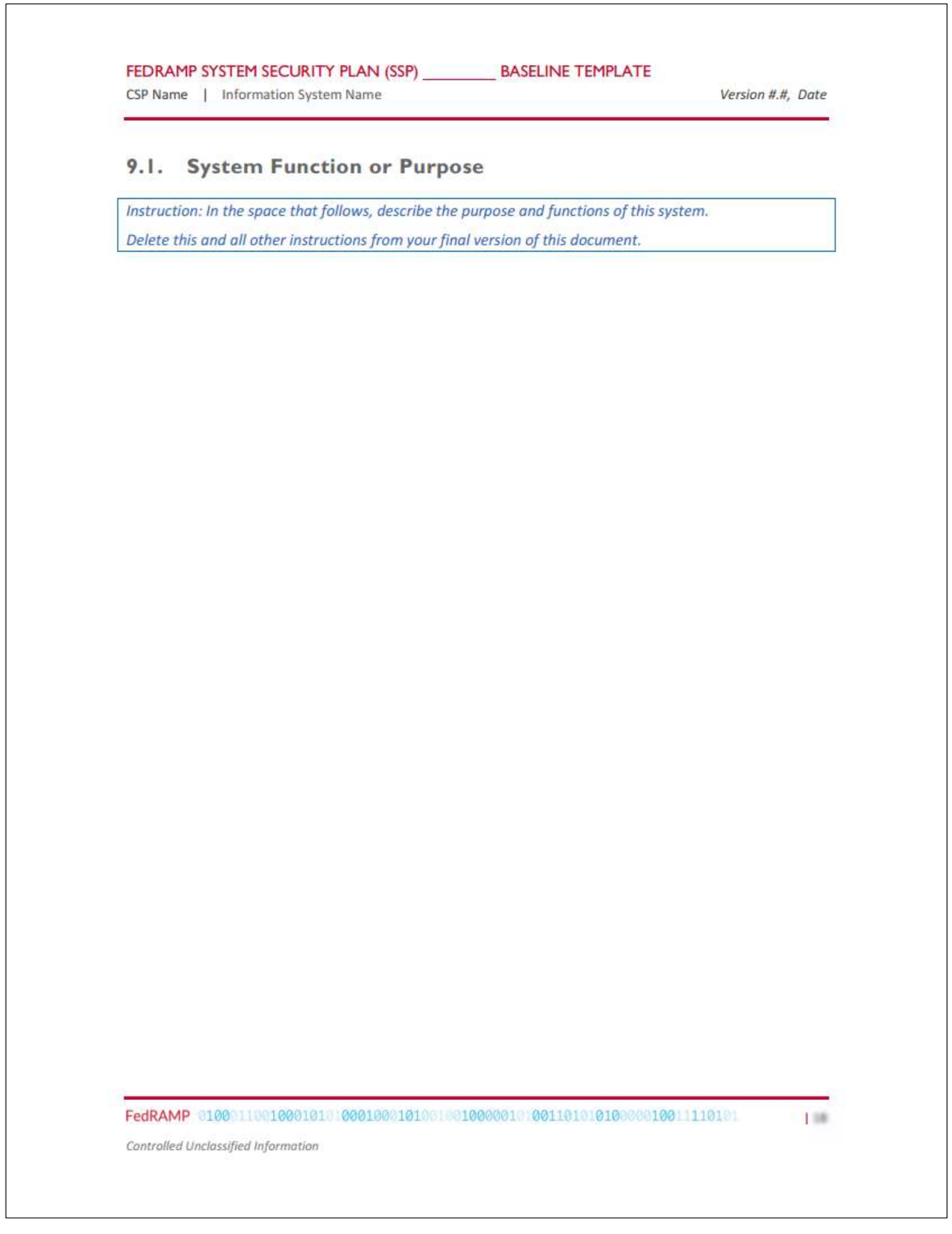
XPath Queries

```
Number of Leveraged Authorizations:
  count(/*/system-implementation/leveraged-authorization)

Name of first leveraged system:
  /*/system-implementation/leveraged-authorization[1]/title

Authorization date of first leveraged system:
  /*/system-implementation/leveraged-authorization[1]/date-authorized
```

Replace "[1]" with "[2]", "[3]", etc.

```
Name of POC for first leveraged system:
  /*/metadata/party[@uuid=/*/system-implementation/leveraged-authorization[1]
  /party-uuid]/name
```

Replace "name" with "email" or "phone" as needed.



9.1. System Function or Purpose

Instruction: In the space that follows, describe the purpose and functions of this system.

Delete this and all other instructions from your final version of this document.

4.16. System Function or Purpose

Representation

```
<system-characteristics>
    <!-- system-name, system-name-short -->
    <description>
        <p>Describe the purpose and functions of this system here.</p>
    </description>
    <!-- prop, link, date-authorized -->
</system-characteristics>
```

XPath Query

```
System Function or Purpose: First paragraph in description
  /*/system-characteristics/description/node()
```

The `description` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/reference/datatypes/ss

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.2. Information System Components and Boundaries

Instruction: In the space that follows, provide an explicit definition of the system's Authorization Boundary. Provide a diagram that portrays this Authorization Boundary and all its connections and components, including the means for monitoring and controlling communications at the external boundary and at key internal boundaries within the system. Address all components and managed interfaces of the information system authorized for operation (e.g., routers, firewalls).

The diagram must include a predominant border drawn around all system components and services included in the authorization boundary. The diagram must be easy to read and understand.

Formal names of components as they are known at the service provider organization in functional specifications, configuration guides, other documents and live configurations shall be named on the diagram and described. Components identified in the Boundary diagram should be consistent with the Network diagram and the inventory(ies). Provide a key to symbols used. Ensure consistency between the boundary and network diagrams and respective descriptions (Section 9.4) and the appropriate Security Controls [AC-20, CA-3(1)].

Additional FedRAMP Requirements and Guidance:

Guidance: *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/

Delete this and all other instructions from your final version of this document.

A detailed and explicit definition of the system authorization boundary diagram is represented in Figure 9-1. Authorization Boundary Diagram below.

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter/resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/back-matter/resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.17. Authorization Boundary Diagram

The OSCAL approach to this type of diagram is to treat the image data as either a linked or base64-encoded `resource` in the `back-matter` section of the OSCAL file, then reference the diagram using the `link` field.

Representation

```
<system-characteristics>
    <!-- leveraged-authorization -->
    <authorization-boundary>
        <description>
            <p>A holistic, top-level explanation of the FedRAMP authorization boundary.</p>
        </description>
        <diagram uuid="uuid-value">
            <description><p>A diagram-specific explanation.</p></description>
            <link href="#uuid-of-boundary-diagram-1" rel="diagram" />
            <caption>Authorization Boundary Diagram</caption>
        </diagram>
        <!-- repeat diagram assembly for each additional boundary diagram -->
    </authorization-boundary>
    <!-- network-architecture -->
</system-characteristics>

<!-- cut -->

<back-matter>
    <resource uuid="uuid-of-boundary-diagram-1">
        <description><p>The primary authorization boundary diagram.</p></description>
        <base64 filename="architecture-main.png" media-type="image/png">00000000</base64>
    </resource>
</back-matter>
```

XPath Queries

```
Overall Description:
  /*/system-characteristics/authorization-boundary/description/node()

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/authorization-boundary/diagram)

Link to First Diagram:
  /*/system-characteristics/authorization-boundary/diagram[1]/link/@href

If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@uuid="uuid-of-boundary-diagram"]/base64
  OR:
  /*/back-matter/resource[@uuid="uuid-of-boundary-diagram-1"]/rlink/@href

Diagram-specific Description:
  /*/system-characteristics/authorization-boundary/diagram[1]/description/node()
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- While resources may generally be linked or embedded, FedRAMP *prefers* the authorization boundary diagram to be embedded (base64).

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

NIST Accepted Values

prop:

- name="type"
  - **Valid:** internal, external, general-public
- name="privilege-type"
  - **Valid:** privileged, non-privileged, no-logical-access

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

See Next Page

4.18. Personnel Roles and Privileges

Representation

```
<metadata>
    <role id="admin-unix">
        <title>Unix Administrator</title>
        <desc>This is a sample role.</desc>
    </role>
</metadata>
<!-- import -->
<!-- system characteristics -->
<system-implementation>
    <!-- prop -->
    <user uuid="uuid-value">
        <title>Unix System Administrator</title>
        <prop name="sensitivity" ns="https://fedramp.gov/ns/oscal" value="limited" />
            <prop name="type" value="external"/>
            <prop name="privilege-level" value="no-logical-access" />
            <role-id>admin-unix</role-id>
            <authorized-privilege>
                <title>Full administrative access (root)</title>
                <function-performed>Add/remove users and hardware</function-performed>
                <function-performed>install and configure software</function-performed>
                <function-performed>OS updates, patches and hotfixes</function-performed>
                <function-performed>perform backups</function-performed>
            </authorized-privilege>
            <!-- for each user repeat authorized-privilege assembly for each privilege -->
    </user>
    <!-- repeat user assembly for each row in Table 9-1 -->
</system-implementation >
```

FedRAMP Extension & Allowed Values

prop (ns="https://fedramp.gov/ns/oscal"):

- name="sensitivity-level"
  - **Valid:** high-risk, severe, moderate, limited, not-applicable

XPath Queries

```
Number of entries in the role table:
  count(/*/system-implementation/user)

Role:
  /*/system-implementation/user[1]/title

Internal or External:
  /*/system-implementation/user[1]/prop[@name="type"]/@value

Privileged, Non-Privileged, or No Logical Access:
  /*/system-implementation/user[1]/prop[@name="privilege-level"]/@value

Sensitivity Level:
  /*/system-implementation/user[1]/prop[@name="sensitivity"][@ns=
  "https://fedramp.gov/ns/oscal"]

Authorized Privileges:
  /*/system-implementation/user[1]/authorized-privilege/title

  count(/*/system-implementation/user[1]/authorized-privilege)

Functions Performed:
  /*/system-implementation/user[1]/authorized-privilege[1]/function-performed[1]

  count(/*/system-implementation/user[1]/authorized-privilege[1]/function-performed)
```

Replace "[1]" with "[2]", "[3]", etc.

NOTE:

- FedRAMP prefers the `authorized-privilege` field be repeated within a user assembly if there is more than one, but will accept all authorized privileges in one field during the early stages of OSCAL adoption.
- FedRAMP prefers separate `function-performed` fields for each function performed but will accept all functions in one field during the early stages of OSCAL adoption.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.3. Types of Users

All personnel have their status categorized with a sensitivity level in accordance with PS-2. Personnel (employees or contractors) of service providers are considered Internal Users. All other users are considered External Users. User privileges (authorization permission after authentication takes place) are described in Table 9-1. Personnel Roles and Privileges that follows.

Instruction: For an External User, write "Not Applicable" in the Sensitivity Level Column. This table must include all roles including systems administrators and database administrators as a role types. (Also include web server administrators, network administrators and firewall administrators if these individuals have the ability to configure a device or host that could impact the CSP service offering.)

This table must also include whether these roles are fulfilled by foreign nationals or systems outside the United States.

Delete this and all other instructions from your final version of this document.

Table 9-1. Personnel Roles and Privileges

Role	Internal or External	Privileged (P), Non-Privileged (NP), or No Logical Access (NLA)	Sensitivity Level	Authorized Privileges	Functions Performed
UNIX System Administrator	Internal	P	Moderate	Full administrative access (root)	Add/remove users and hardware, install and configure software, OS updates, patches and hotfixes, perform backups
Client Administrator	External	NP	N/A	Portal administration	Add/remote client users. Create, modify and delete client applications
Program Director	Internal	NLA	Limited	N/A	Reviews, approves and enforces policy
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		
	Choose an item.	Choose an item.	Choose an item.		

See Previous Page

There are currently <number> internal personnel and <number> external personnel. Within one year, it is anticipated that there will be <number> internal personnel and <number> external personnel.

4.19. Number of Users

The Core OSCAL syntax does not provide fields for the number of internal and external uses. These current and future values are handled as FedRAMP Extensions.

Representation

```
<system-implementation>
    <prop name="users-internal" ns="https://fedramp.gov/ns/oscal" value="22"/>
    <prop name="users-external" ns="https://fedramp.gov/ns/oscal" value="110"/>
    <prop name="users-internal-future" ns="https://fedramp.gov/ns/oscal" value="25"/>
    <prop name="users-external-future" ns="https://fedramp.gov/ns/oscal" value="200"/>
</system-implementation>
```

FedRAMP Extensions

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="users-internal"`
- `name="users-external"`
- `name="users-internal-future"`
- `name="users-external-future"`

XPath Queries

```
Number of current internal users:
  /*/system-implementation/prop[@name="users-internal"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Number of current external users:
  /*/system-implementation/prop[@name="users-external"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Number of future internal users (1 year):
  /*/system-implementation/prop[@name="users-internal-future"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Number of future external users (1 year):
  /*/system-implementation/prop[@name="users-external-future"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

11. SYSTEM INTERCONNECTIONS

FedRAMP Extensions & Allowed Values

prop
(`ns="https://fedramp.gov/ns/oscal"`):

- `name="service-processor"`
- `name="information`
- `name="port"`
- `name="circuit"`

prop
(`ns="https://fedramp.gov/ns/oscal"`):

- `name="connection-security"`
  - **Valid:** `ipsec, vpn, ssl, certificate, secure-file-transfer, other`

address and interface … and the IP address of … urity, indicate how the … Being Transmitted, des… r. Add additional rows

Cloud Service Provider

NIST Allowed Values

Required ICA Role IDs:

- `isa-poc-remote`
- `isa-poc-local`
- `isa-authorizing-official-remote`
- `isa-authorizing-official-local`

on of this document.

with Table 13-3 CA-3 Authorized Connections.

le 11-1. System Interconnections

	Address of System	int of Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/datatypes/#markup-multiline

Table 13-3. CA-3 Authorized Connections

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>

4.20. System Interconnections and Authorized Connections (Representation)

Table 11-1 and Table 13-3 are closely related and modeled together in OSCAL.

Representation

```
<metadata>
    <!-- oscal-version, prop -->
    <role id="isa-poc-remote">
        <title>Remote System POC</title>
    </role>
    <!-- repeat role assembly for each required ICA role ID -->
    <party uuid="uuid-value" type="organization">
        <name>Remote Organization</name>
    </party>
    <party uuid="uuid-value">
        <name>Remote POC's Name</name>
        <email>person@ica.example.com</email>
        <phone>202-555-1212</phone>
        <member-of-organization>uuid-of-remote-organization-party</member-of-organization>
    </party>
    <!-- repeat party assembly for each ICA POC -->
</metadata>
<!-- import-profile, system-characteristics -->
    <component uuid="uuid-value" type="interconnection">
        <title>[EXAMPLE]Authorized Connection System Name</title>
        <prop name="service-processor" ns="https://fedramp.gov/ns/oscal" value="Telco Name"/>
        <prop name="ipv4-address" class="local" value="10.1.1.1"/>
        <prop name="ipv4-address" class="remote" value="10.2.2.2"/>
        <prop name="interconnection-direction" value="ingoing-outgoing"/>
        <prop name="information" ns="https://fedramp.gov/ns/oscal"
              value="A summary and the type of information transmitted, such as 800-62 Rev. 2
Volume 1 information types."/>
        <protocol name="http">
            <port-range start="80" end="80" transport="TCP"/>
        </protocol>
        <protocol name="https">
            <port-range start="443" end="443" transport="TCP"/>
        </protocol>
        <prop name="interconnection-security" ns="https://fedramp.gov/ns/oscal"
              value="ipsec"/>
        <link href="#uuid-of-ICA-resource-in-back-matter" rel="isa-greement" />
        <!-- repeat responsible-party assembly for each required ICA role id -->
        <responsible-role role-id="isa-poc-remote">
            <party-id>isa-1</party-id>
        </responsible-role>
        <remarks><p>Optional notes about this interconnection</p></remarks>
    </component>
    <!-- repeat interconnection assembly for each ICA -->
    <!-- control-implementation -->
<back-matter>
    <resource uuid="uuid-value">
        <title>[SAMPLE]Interconnection Security Agreement Title</title>
        <prop name="version" value="Document Version"/>
        <rlink href="./documents/ISAs/ISA-1.docx"/>
        <citation><!-- cut --></citation>
    </resource>
    <!-- repeat citation assembly for each ICA -->
</back-matter>
```

SEE NEXT PAGE FOR QUERIES

4.21. System Interconnections and Authorized Connections (Queries)

11. SYSTEM INTERCONNECTIONS

Instruction: List all interconnected systems. Provide the IP address and interface identifier (eth0, eth1, eth2) for the CSP system that provides the connection. Name the external organization and the IP address of the external system. Provide a point of contact and phone number for the external organization. For Connection Security, indicate how the connection is being secured. For Data Direction, indicate which direction the packets are flowing. For Information Being Transmitted, describe what type of data is being transmitted. If a dedicated telecom line is used, indicate the circuit number. Add additional rows as needed. This table must be consistent with Table 13-3 CA-3 Authorized Connections.

Additional FedRAMP Requirements and Guidance:

Guidance: *See the FedRAMP Documents page under Key Cloud Service Provider (CSP) Documents> FedRAMP Authorization Boundary Guidance*
https://www.fedramp.gov/documents/

Delete this and all other instructions from your final version of this document.

Table 11-1 System Interconnections below is consistent with Table 13-3 CA-3 Authorized Connections.

Table 11-1. System Interconnections

SP* IP Address and Interface	External Organization Name and IP Address of System	External Point of Contact and Phone Number	Connection Security (IPSec VPN, SSL, Certificates, Secure File Transfer, etc.)**	Data Direction (incoming, outgoing, or both)	Information Being Transmitted	Port or Circuit Numbers
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>
<SP IP Address/Interface>	<External Org/IP>	<External Org POC> <Phone 555-555-5555>	<Enter Connection Security>	Choose an item.	<Information Transmitted>	<Port/Circuit Numbers>

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

Table 13-3. CA-3 Authorized Connections

Authorized Connections Information System Name	Name of Organization CSP Name System Connects To	Role and Name of Person Who Signed Connection Agreement	Name and Date of Interconnection Agreement
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections System Name>	<Name Org CSP System Connects To>	<Role and Name Signed Connection Agreement>	<Name and Date of Interconnection Agreement>
<Authorized Connections	<Name Org CSP System	<Role and Name Signed	<Name and Date of

Queries are for the Interconnection Security Agreement (ISA)'s remote POC and AO information. To obtain the ISA's local POC and AO information:

```
Replace "isa-poc-remote" with "isa-poc-local"
Replace "[isa-authorizing-official-remote" with "isa-authorizing-official-local"
```

XPath Queries

```
Replace "[1]" with "[2]", "[3]", etc.
```

```
(11-1) Service Processor (SP):
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="service-
  processor"][@ns="https://fedramp.gov/ns/oscal"]/@value
(11-1) IP Address and Interface:
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="ipv4-
  address"][@class="local"]/@value
(11-1) External Organization Name ...:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=/*/system-implementation/component
  [@type='interconnection'][1]/responsible-role/party-uuid]/member-of-organization]/name
AND IP Address of System:
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="ipv4-
  address"][@class="remote"]
(11-1)External Point of Contact:
  /*/metadata/party[@uuid=/*/system-implementation/component[@type='interconnection']
  [1]/responsible-role[@role-id='isa-poc-remote']/party-uuid]/name
AND Phone Number:
  /*/metadata/party[@uuid=/*/system-implementation/component[@type='interconnection']
  [1]/responsible-role[@role-id='isa-poc-remote']/party-uuid]/telephone-number
(11-1) Connection Security:
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="connection-
  security"][@ns="https://fedramp.gov/ns/oscal"]/@value
(11-1) Connection Security - Remark (required if "other"):
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="connection-
  security"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()
(11-1)Data Direction (may be more than one result):
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="direction"]
(11-1) Information Being Transmitted:
  /*/system-implementation/component[@type='interconnection'][1]
  /prop[@name="information"][@ns="https://fedramp.gov/ns/oscal"]/@value
(11-1)Port or Circuit Numbers:
  /*/system-implementation/component[@type='interconnection'][1]/prop[@name="port" or
  @name="circuit"][@ns="https://fedramp.gov/ns/oscal"]/@value
(13-3) Authorized Connections Information System Name:
  /*/system-implementation/component[@type='interconnection'][1]/title
(13-3)Name of Organization CSP Name System Connects To [same as (11-1) External Org Name]:
  /*/metadata/party[@uuid=/*/metadata/party[@uuid=/*/system-
  implementation/component[@type='interconnection'][1]/responsible-role[@role-id='isa-poc-
  remote']/party-uuid]/member-of-organization]/name
(13-3) Role of Person Who Signed Connection Agreement (Remote)
  /*/metadata/party[@uuid=/*/system-implementation/component[@type=
  'interconnection'][1]/responsible-role[@role-id='isa-authorizing-official-remote']
  /party-uuid]/prop[@name="job-title"]/@value
(13-3) Name of Person Who Signed Connection Agreement (Remote) [same as (11-1)]
  /*/metadata/party[@uuid=/*/system-implementation/component[@type=
  'interconnection'][1]/responsible-role[@role-id='isa-authorizing-official-remote']/party-
  uuid]/name
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

9.4. Network Architecture

Instruction: Insert a network architectural diagram in the space that follows. Ensure that the following items are labeled on the diagram: hostnames, Domain Name System (DNS) servers, DHCP servers, authentication and access control servers, directory servers, firewalls, routers, switches, database servers, major applications, storage, Internet connectivity providers, telecom circuit numbers, network interfaces and numbers, VLANs. Major security components should be represented. If necessary, include multiple network diagrams.

Delete this and all other instructions from your final version of this document.

Assessors should be able to easily map hardware, software and network inventories back to this diagram.

The logical network topology is shown in Figure 9-2. Network Diagram mapping the data flow between components.

The following Figure 9-2. Network Diagram(s) provides a visual depiction of the system network components that constitute Enter Information System Abbreviation.

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter\resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/</resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.22. Network Architecture Diagram(s)

Representation

```
<system-characteristics>
    <!-- authorization-boundary -->
    <network-architecture>
        <description>
            <p>A holistic, top-level explanation of the system's network.</p>
        </description>
        <diagram uuid="uuid-value">
            <description><p>A diagram-specific explanation.</p></description>
            <link href="#uuid-of-network-diagram-1" rel="diagram" />
            <caption>Network Diagram</caption>
        </diagram>
        <!-- repeat diagram assembly for each additional network diagram -->
    </network-architecture>
    <!-- data-flow -->
</system-characteristics>


<!-- cut -->


<back-matter>
    <!-- citation -->
    <resource uuid=" uuid-of-network-diagram-1">
        <description><p>The primary network architecture diagram.</p></description>
        <rlink href="./diagrams/network.png" media-type="image/png"/>
    </resource>
</back-matter>
```

XPath Queries

```
Overall Description:
  /*/system-characteristics/network-architecture/description/node()

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/network-architecture/diagram)

Link to First Diagram:
  /*/system-characteristics/network-architecture/diagram[1]/link/@href

                                                  Replace "[1]" with "[2]", "[3]", etc.


If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@uuid="uuid-of-network-diagram-1"]/base64
  OR:
  /*/back-matter/resource[@uuid="uuid-of-network-diagram-1"]/rlink/@href

First Diagram Description:
  /*/system-characteristics/network-architecture/diagram[1]/description/node()
```

NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the network architecture diagrams to be embedded (base64).

10. SYSTEM ENVIRONMENT AND INVENTORY

Directions for attaching the FedRAMP Inventory Workbook may be found in the following section: Attachment 13, FedRAMP Inventory Workbook.

Instruction: In the space that follows, provide a general description of the technical system environment. Include information about all system environments that are used, e.g., production environment, test environment, staging or QA environments. Include the specific location of the alternate, backup and operational facilities.

In your description, also include a reference to Attachment 13, the system's Integrated Inventory Workbook, which should provide a complete listing of the system's components (operating systems/infrastructure, web applications/software, and databases). The Integrated Inventory Workbook should be maintained and updated monthly by the CSP, as part of continuous monitoring efforts. Instructions for completing the Integrated Inventory Workbook are provided within the Integrated Inventory Workbook.

Delete this and all other instructions from your final version of this document.

4.23. Data Center Locations

Representation

```
<metadata>
    <!-- role  -->
    <location uuid="uuid-of-data-center-location-1">
        <title>Primary Processing Site</title>
        <address>
            <addr-line>2222 Main Street</addr-line>
            <city>Anywhere</city>
            <state>--</state>
            <postal-code>00000-0000</postal-code>
        </address>
        <prop name="type" class="primary" value="data-center"/>
    </location>

    <location uuid="uuid-of-data-center-location-2">
        <title>Alternate Processing Site</title>
        <address>
            <addr-line>3333 Small Road</addr-line>
            <city>Anywhere</city>
            <state>--</state>
            <postal-code>00000-0000</postal-code>
        </address>
        <prop name="type" class="alternate" value="data-center"/>
    </location>
</metadata>
```

XPath Queries

```
List of Processing Sites (Data Centers):
  /*/metadata/location[prop[@name='type'][@value='data-center']]/title

Number of Processing Sites (integer):
  count(/*/metadata/location[prop[@name='type'][@value='data-center']])

List of Primary Processing Sites:
  /*/metadata/location[prop[@name='type'][@class='primary'][@value='data-center']]/title

Number of Primary Processing Sites (integer):
  count(/*/metadata/location[prop[@name='type'][@class='primary'][@value='data-center']])

Street Address of First Processing Site:
  (/*/metadata/location[prop[@name='type'][@value='data-center']])[1]/address/addr-line

Street Address of First Primary Processing Site:
  (/*/metadata/location[prop[@name='type'][@class='primary'][@value='data-
  center']])[1]/address/addr-line
```

NOTE:

- Replace "`[1]`" with "`[2]`", "`[3]`", etc.
- Replace "`addr-line`" with "`city`", "`state`", or "`postal-code`" as needed for the remainder of the address.
- Replace "`primary`" with "`alternate`" for alternate processing site.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

10.1. Data Flow

Instruction: In the space that follows, describe the flow of data in and out of system boundaries and insert a data flow diagram. Describe protections implemented at all entry and exit points in the data flow as well as internal controls between customer and project users. Include data flows for privileged and non-privileged authentication/authorization to the system for internal and external users. If necessary, include multiple data flow diagrams.

Delete this and all other instructions from your final version of this document.

The data flow in and out of the system boundaries is represented in Figure 10-1. Data Flow Diagram, below.

Figure 10-1. Data Flow Diagram

In OSCAL, the `link` field's `href` flag may be any URI that points to the actual diagram image file; however, FedRAMP requires the authorization boundary, network, and data flow diagrams to be embedded or attached via `back-matter\resource` assemblies. This means the `href` flag should always be a URI fragment (#diagram-id). FedRAMP tools must recognize the fragment, and locate the appropriate resource using the diagram ID. (`/*/back-matter/resource[@id='diagram-id']`)

The `description` fields are *Markup multiline* and the `caption` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

FedRAMP has not yet established image format standards for the authorization boundary, network, and dataflow diagrams. Please use a format that will render natively in most modern browsers, and ensure the image quality is high enough to read all text when zoomed in.

4.24. Data Flow Diagrams

Representation

```
<system-characteristics>
    <!-- network-architecture -->
    <data-flow>
        <description>
            <p>A holistic, top-level explanation of the system's data flows.</p>
        </description>
        <diagram uuid="uuid-value">
            <description><p>A diagram-specific explanation.</p></description>
            <link href="#uuid-of-dataflow-diagram-1" rel="diagram" />
            <caption>Data Flow Diagram</caption>
        </diagram>
        <!-- repeat diagram assembly for each additional data flow diagram -->
    </data-flow>
    <!-- network-architecture -->
</system-characteristics>

<!-- cut -->

<back-matter>
    <!-- citation -->
    <resource uuid="uuid-of-network-diagram-1">
        <description><p>The primary data flow diagram.</p></description>
        <base64 filename="data-flow-1.png" media-type="image/png">
            0000<!-- base64 cut -->0000
        </base64>
    </resource>
</back-matter>
```

XPath Queries

```
Overall Description:
  /*/system-characteristics/data-flow/description/node()

Count the Number of Diagrams (There should be at least 1):
  count(/*/system-characteristics/data-flow/diagram)

Link to First Diagram:
  /*/system-characteristics/data-flow/diagram[1]/link/@href

                                          Replace "[1]" with "[2]", "[3]", etc.

If the diagram link points to a resource within the OSCAL file:
  /*/back-matter/resource[@uuid="uuid-of-dataflow-diagram-1"]/base64
  OR:
  /*/back-matter/resource[@uuid="uuid-of-dataflow-diagram-1"]/rlink/@href

First Diagram Description:
  /*/system-characteristics/data-flow/diagram[1]/description/node()
```

NOTE:

- While resources may generally be linked or embedded, FedRAMP prefers the data flow diagrams to be embedded (base64).

10.2. Ports, Protocols and Services

The Table 10-1. Ports, Protocols and Services below lists the ports, protocols and services enabled in this information system.

Instruction: In the column labeled "Used By" please indicate the components of the information system that make use of the ports, protocols and services. In the column labeled "Purpose" indicate the purpose for the service (e.g., system logging, HTTP redirector, load balancing). This table should be consistent with CM-6 and CM-7. You must fill out this table, even if you are leveraging a pre-existing FedRAMP Authorization. Add more rows as needed.

Delete this and all other instructions from your final version of this document.

Table 10-1. Ports, Protocols and Services

Ports (TCP/UDP)*	Protocols	Services	Purpose	Used By
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>
<Enter Port>	<Enter Protocols>	<Enter Services>	<Enter Purpose>	<Enter Used By>

* Transmission Control Protocol (TCP), User Diagram Protocol (UDP)

The `description` fields are *Markup multiline* and the `purpose` field is *Markup-line*. These enable the text to be formatted, which requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

NIST has consolidated OSCAL syntax and is now handling ports, protocols and services as components. This is a change from the SSP Syntax in Milestone Release 2.

4.25. Ports, Protocols and Services

Entries in the ports, protocols, and services table are represented as `component` assemblies, with the `component-type` flag set to "`service`". Use a `protocol` assembly for each protocol associated with the service. For a single port, set the port-range `start` flag and `end` flag to the same value.

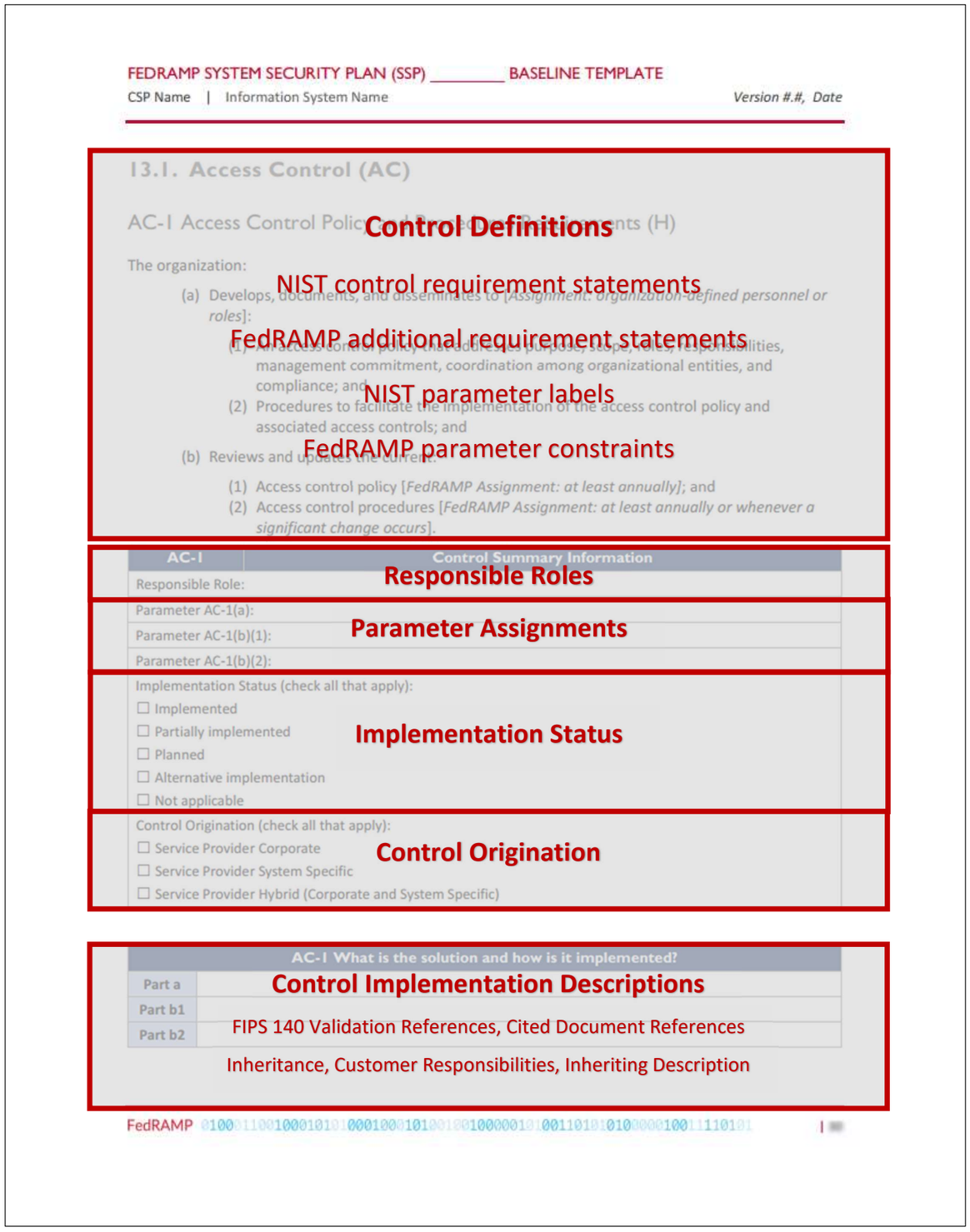
Representation

```
<system-implementation>
    <!-- user -->
    <component uuid="uuid-of-service" type="service">
        <title>[SAMPLE]Service Name</title>
        <description><p>Describe the service</p></description>
        <purpose>Describe the purpose the service is needed.</purpose>
        <prop name="used-by" value="What uses this service?"/>
            <status state="operational" />
            <protocol name="http">
                <port-range start="80" end="80" transport="TCP"/>
            </protocol>
            <protocol name="https">
                <port-range start="443" end="443" transport="TCP"/>
            </protocol>
    </component>
    <!-- Repeat the component assembly for each row in Table 10-1 -->
    <!-- system-inventory -->
</system-implementation>
```

XPath Queries

```
Number of entries in the Ports, Protocols and Services table:
  count(/*/system-implementation/component[@type='service'])

Number of protocols specified (1st service):
  count(/*/system-implementation/component[@type='service'][1]/protocol)

Number of port ranges specified (1st service, 1st protocol):
  count(/*/system-implementation/component[@type='service'][1]/protocol[1]/port-range)

Ports: Start (1st service, 1st protocol, 1st port range):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/port-range[1]/@start

Ports: End (1st service, 1st protocol, 1st port range):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/port-range[1]/@end

Ports: Transport (1st service, 1st protocol, 1st port range):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/port-range[1]/@transport

Protocol (1st service, 1st protocol):
  /*/system-implementation/component[@type='service'][1]/protocol[1]/@name

Service (1st service):
  /*/system-implementation/component[@type='service'][1]/title

Purpose (1st service):
  /*/system-implementation/component[@type='service'][1]/purpose

Used By (1st service):
  /*/system-implementation/component[@type='service'][1]/prop[@name="ce"]
```

Replace "[1]" with "[2]", "[3]", etc.



5. SECURITY CONTROLS

This section describes the modeling of security control information in an OSCAL-based FedRAMP SSP. To ensure consistent processing, FedRAMP imposes specific requirements on the use of OSCAL for control implementation information.

The modeling of controls is addressed in the following sections as follows:

- **Section 5.1, Control Definitions**
- **Section 5.2, Responsible Roles Responsible Roles** and Parameter Assignments
- **Section 5.3, Implementation Status**
- **Section 5.3.1.1, Control Origination**
- **Section 5.4, Control Implementation Descriptions**
    - **Organization**
        - **Policy and Procedure Statements**
        - **Multi-Part Statements**
        - **Single Statements**
    - **Response**
        - **Overview**
        - **Example**
        - **"This System"**
        - **Inheriting from a Leveraged Authorization**
        - **Identifying Customer Responsibilities**
        - **Providing Inheritance**

This section provides the preferred approach to representing controls in OSCAL. For system owners converting their MS Word-based SSP to OSCAL, see *Appendix B, Converting a Legacy SSP to* OSCAL for an alternative OSCAL control representation, which aligns better with legacy SSP content.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-8 System Use Notification (L) (M) (H)

The information system:

(a) Displays to users [*Assignment: organization-defined system use notification message or banner (FedRAMP Assignment: see additional Requirements and Guidance)*] before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:

(1) Users are accessing a U.S. Government information system;
(2) Information system usage may be monitored, recorded, and subject to audit;
(3) Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and
(4) Use of the information system indicates consent to monitoring and recording;

(b) Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and

(c) For publicly accessible systems:

(1) Displays system use information [*Assignment: organization-defined conditions (FedRAMP Assignment: see additional Requirements and Guidance)*], before granting further access;
(2) Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
(3) Includes a description of the authorized uses of the system.

AC-8 Additional FedRAMP Requirements and Guidance:

Requirement: The service provider shall determine elements of the cloud environment that require the System Use Notification control. The elements of the cloud environment that require System Use Notification are approved and accepted by the JAB/AO.

Requirement: The service provider shall determine how System Use Notification is going to be verified and provide appropriate periodicity of the check. The System Use Notification verification and periodicity are approved and accepted by the JAB/AO.

Guidance: If performed as part of a Configuration Baseline check, then the % of items requiring setting that are checked and that pass (or fail) check can be provided.

Requirement: If not performed as part of a Configuration Baseline check, then there must be documented agreement on how to provide results of verification and the necessary periodicity of the verification by the service provider. The documented agreement on how to provide verification of the results are approved and accepted by the JAB/AO.

5.1. Control Definitions

All control definition information is imported from the appropriate FedRAMP baseline (OSCAL profile). This includes the original NIST control definition and parameter labels, as well as any FedRAMP control guidance, and parameter constraints.

Interpreting and presenting profile content is beyond the scope of this document. Please refer to the NIST OSCAL Profile and Catalog schema references for more information:

- Profile Model
- Catalog Reference

Only the control implementation information is present within an OSCAL-based SSP. Each control in the FedRAMP baseline must have a corresponding `implemented-requirement` assembly in the `control-implementation` assembly.

Representation

```
<!-- metadata -->
<import-profile href="https://path/to/xml/FedRAMP_MODERATE-baseline_profile.xml"/>
<!-- system-characteristics -->
<!-- system-implementation -->
<control-implementation>
    <description>
        <p>This field required by OSCAL, but may be left blank.</p>
        <p>FedRAMP requires no specific content here.</p>
    </description>

    <!-- one implemented-requirement assembly for each required control -->
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <!-- Control content cut - See next pages for detail -->
    </implemented-requirement>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
    <!-- Control content cut - See next pages for detail -->
    </implemented-requirement>
    <implemented-requirement uuid="uuid-value" control-id="ac-2.1">
    <!-- Control content cut - See next pages for detail -->
    </implemented-requirement>

</control-implementation>
<!-- back-matter -->
```

XPath Queries

Replace "ac-1" with target control ID.

```
URI to Profile:
  /*/import-profile/@href

CSP's Control Implementation Information
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]
```

NOTE:

- FedRAMP tools check to ensure there is one `implemented-requirement` assembly for each control identified in the applicable FedRAMP baseline.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	

Implementation Status (check all that apply):

- ☐ Implemented
- ☐ Partially implemented
- ☐ Planned
- ☐ Alternative implementation
- ☐ Not applicable

Control Origination (check all that apply):

- ☐ Service Provider Corporate
- ☐ Service Provider System Specific
- ☐ Service Provider Hybrid (Corporate and System Specific)
- ☐ Configured by Customer (Customer System Specific)
- ☐ Provided by Customer (Customer System Specific)
- ☐ Shared (Service Provider and Customer Responsibility)
- ☐ Inherited from pre-existing FedRAMP Au… enter text. , Date of Authorization

See Next Pages

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

5.2. Responsible Roles and Parameter Assignments

Every applicable control must have at least one `responsible-role` defined. There must be a separate `responsible-role` assembly for each responsible role. OSCAL requires the specified `role-id` to be valid in the defined list of `roles` in the `metadata`. Controls with a FedRAMP `implementation-status` property value of `non-applicable` (see section 5.3) do not require a `responsible-role`. FedRAMP further requires the specified `role-id` must also have been referenced in the `system-implementation`/`user` assembly. This equates to the FedRAMP requirement of all responsible roles appearing in the Personnel Roles and Privileges table.

With the `implemented-requirement` assembly, there must be one `set-parameter` statement for each of the control's parameters, as specified in the FedRAMP baseline and illustrated in the example representation below. The only exception to this is with nested parameters. Some select parameters contain an assignment parameter within a selection parameter, such as appears in AC-7 (b). In these instances, only the final selected value must be provided. The nested assignment parameter may be ignored.

OSCAL also supports parameter setting at the component level, within a `by-component` assembly.

Representation

```
<metadata>
    <role id="admin-unix">
        <title>Unix Administrator</title>
    </role>
</metadata>
<!-- Fragment: -->
<system-implementation>
    <user uuid="uuid-value">
        <role-id>admin-unix</role-id>
    </user>
</system-implementation >
<!-- system-implementation -->
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <!-- cut -->
        <responsible-role role-id="admin-unix" />
        <set-parameter param-id="ac-2_prm_1">
            <value>System Manager, System Architect, ISSO</value>
        </set-parameter >
        <!-- cut -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

Replace "ac-2" with target control ID.

```
Number of specified Responsible Roles:
  count(/*/control-implementation/implemented-requirement[@control-id="ac-2"]/
  responsible-role)
```

Replace "[1]" with "[2]", "[3]", etc.

```
Responsible Role:
  /*/metadata/role[@id=/*/control-implementation/implemented-requirement
  [@control-id="ac-2"]/responsible-role[1]/@role-id]/title

Check for existence in Personnel Roles and Privileges (Should return a number > 0)
  count(/*/system-implementation/user/role-id[string(.)=/*/control-implementation/
  implemented-requirement[@control-id="ac-2"]/responsible-role/@role-id])

Parameter Value:
  /*/control-implementation/implemented-requirement[@control-id="ac-2"]/set-parameter
  [@param-id="ac-2_prm_1"]/value
```

Replace "ac-2_prm_1" with target parameter ID.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	

See Previous Page

Implementation Status (check all that apply):

- ☐ Implemented
- ☐ Partially implemented
- ☐ Planned
- ☐ Alternative implementation
- ☐ Not applicable

Control Origination (check all that apply):

- ☐ Service Provider Corporate
- ☐ Service Provider System Specific
- ☐ Service Provider Hybrid (Corporate and System Specific)
- ☐ Configured by Customer (Customer System Specific)
- ☐ Provided by Customer (Customer System Specific)
- ☐ Shared (Service Provider and Customer Responsibility)
- ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization

AC-2 What is the solution and how is it implemented?
Part a
Part b
Part c
Part d
Part e
Part f

See Next Pages

FedRAMP Extensions and Accepted Values

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="planned-completion-date"`

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="implementation-status"`
  Valid: `implemented, partial, planned, alternative, not-applicable`

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

5.3. Implementation Status

FedRAMP only accepts only one of five values for `implementation-status`: `implemented`, `partial`, `planned`, `alternative`, and `not-applicable`. A control may be marked "partial" and "planned" (using two separate `implementation-status` fields). All other choices are mutually exclusive.

If the implementation-status is `partial`, the gap must be explained in the `remarks` field.

If the implementation-status is `planned`, a brief description of the plan to address the gap, including major milestones must be explained in the `remarks` field. There must also be a prop (`name="planned-completion-date" ns="https://fedramp.gov/ns/oscal")` field containing the intended completion date. With XML, `prop` fields must appear before `prop` fields, even though that sequence is counter-intuitive in this situation.

If the implementation-status is `alternative`, the alternative implementation must be summarized in the `remarks` field.

If the implementation-status is `not-applicable`, the N/A justification must be provided in the `remarks` field.

Implementation Status Representation

```
<!-- system-implementation -->
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <prop name="planned-completion-date"
            ns="https://fedramp.gov/ns/oscal" value="2021-01-01Z"/>
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="implemented" />
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="partial" />
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="planned" />
        <prop name="implementation-status"
            ns="https://fedramp.gov/ns/oscal" value="not-applicable"/>
        <!-- responsible-role, statement, by-component -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

Implementation Status XPath Queries

Replace "ac-1" with target control-id.

```
Implementation Status (may return more than 1 result for a given control):
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]
  /prop[@name="implementation-status"]/@value

Gap Description (If implementation-status="partial"):
  /*/control-implementation/implemented-requirement/prop[@name='implementation-
  status'][@value="partial"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()

Planned Completion Date (If implementation-status="planned"):
  /*/control-implementation/implemented-requirement[@control-id="ac-1"]/
  prop[@name="planned-completion-date"][@ns="https://fedramp.gov/ns/oscal"]/@value

Plan for Completion (If implementation-status="planned"):
  /*/control-implementation/implemented-requirement/prop[@name='implementation-
  status'][@value="planned"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()

Not Applicable (N/A) Justification (If implementation-status="na"):
  /*/control-implementation/implemented-requirement/prop[@name='implementation-
  status'][@value="not-applicable"][@ns="https://fedramp.gov/ns/oscal"]/remarks/node()
```

The FedRAMP `implementation-status` property at the control's `implemented-requirement` level is a summary of all statement and/or component level core OSCAL `implementation-status` designations. It must be set to the appropriately based on the least value of child statement or component level `implementation-status` designations. When a statement and/or component level `implementation-status` designation is not specified, the FedRAMP `implementation-status` value is assumed. Individual statements and/or components may override `implementation-status` locally.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply):	
☐ Implemented	
☐ Partially implemented	
☐ Planned	
☐ Alternative implementation	
☐ Not applicable	
Control Origination (check all that apply):	
☐ Service Provider Corporate	
☐ Service Provider System Specific	
☐ Service Provider Hybrid (Corporate and System Specific)	
☐ Configured by Customer (Customer System Specific)	
☐ Provided by Customer (Customer System Specific)	
☐ Shared (Service Provider and Customer Responsibility)	
☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text., Date of Authorization	

See Previous Pages

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	

See Next Pages

FedRAMP Extensions and Accepted Values

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="control-origination"`
  Valid: `sp-corporate, sp-system, customer-configured, customer-provided, inherited`

Instead of hybrid, identify multiple control-origination types, each in its own `prop` assembly.

The `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

5.3.1.1. Control Origination

FedRAMP accepts only one of five values for `control-origination`: `sp-corporate`, `sp-system`, `customer-configured`, `customer-provided`, and `inherited`. Hybrid choices are now expressed by identifying more than one `control-origination`, each in a separate prop field.
For controls with a control-id ending in "-1", FedRAMP only accepts `sp-corporate`, and `sp-system`.

If the control origination is `inherited`, there must also be a FedRAMP extension (`prop name="leveraged-authorization-uuid" ns="https://fedramp.gov/ns/oscal"`) field containing the UUID of the leveraged authorization as it appears in the `/*/system-implementation/leveraged-authorization` assembly.

Control Origination Representation

```
<system-implementation>
    <!-- status -->
    <leveraged-authorization uuid="uuid-of-leveraged-authorization">
        <!-- details cut - see Leveraged Authorizations Section -->
    </leveraged-authorization>
</system-implmentation>

<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <prop name="leveraged-authorization-uuid"
            value="uuid-of-leveraged-authorization"/>
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="sp-corporate" />
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="sp-system" />
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="customer-configured" />
        <prop ns="https://fedramp.gov/ns/oscal" name="control-origination"
            value="inherited" />
        <!-- responsible-role -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

```
Number of Control Originations:
  count(/*/control-implementation/implemented-requirement[@control-id="ac-2"]/
  prop[@name="control-origination"][@ns="https://fedramp.gov/ns/oscal"])

Control Origination(could return more than 1 result):
  /*/control-implementation/implemented-requirement[@control-id="ac-2"]/prop
  [@name="control-origination"][@ns="https://fedramp.gov/ns/oscal"][1]/@value

Inherited From: System Name (If control-origination="inherited"):
  /*/system-implementation/leveraged-authorization[@uuid=/*/control-implementation/
  implemented-requirement[@control-id="ac-2"]/prop[@name="leveraged-authorization-
  uuid"]]/title

Inherited From: Authorization Date (If control-origination="inherited"):
  /*/system-implementation/leveraged-authorization[@uuid=/*/control-implementation/
  implemented-requirement[@control-id="ac-2"]/prop[@name="leveraged-authorization-
  uuid"]]/date-authorized
```

Replace "[1]" with "[2]", "[3]", etc.

Policy and Procedure Statements

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

Multi-Part Statements

The organization:

(a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];

(b) Assigns account managers for information system accounts;

cut c, d, e, f, g, h, i

(j) Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: monthly for privileged accessed, every six (6) months for non-privileged access*]; and

(k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

Single Statement

The organization employs automated mechanisms to support the management of information system accounts.

AC-2 (1) What is the solution and how is it implemented?

5.4. Control Implementation Descriptions

Within the OSCAL-based FedRAMP baselines, control statements and control objectives are tagged with a `response-point` FedRAMP Extension. Every control statement designated as a `response-point` in the baseline must have a `statement` with the control's `implemented-requirement` assembly. Please note control objective response points are used for the SAP and SAR.

When using a **FedRAMP Resolved Profile Catalog**, the following query will identify the response points for a given control.

XPath Query

```
Response Points for AC-1:
  //control[@id='ac-1']/part[@name='statement']//prop[@name='response-
  point'][@ns='https://fedramp.gov/ns/oscal']/../@id
```

Replace "ac-1" with other control IDs as required.

5.4.1. Organization: Policy and Procedure Statements

For each of the -1 controls, such as AC-1, there must be exactly four `statement` assemblies: Part (a)(1), Part (a)(2), Part (b)(1) and Part (b)(2).

Policy and Procedure Representation

```
<!-- system-implementation -->
<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <statement statement-id="ac-1_smt.a.1"><!-- cut --></statement>
        <statement statement-id="ac-1_smt.a.2"><!-- cut --></statement>
        <statement statement-id="ac-1_smt.b.1"><!-- cut --></statement>
        <statement statement-id="ac-1_smt.b.2"><!-- cut --></statement>
    </implemented-requirement>
</control-implementation>
```

5.4.2. Organization: Multi-Part Statements:

There must be one `statement` assembly for each lettered part, such as with AC-2, parts a, b, c, etc.

Multi-Part Statement Representation

```
<!-- system-implementation -->
<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement statement-id="ac-2_smt.a"><!-- cut --></statement>
        <!-- repeat for b, c, d, e, f, g, h, i, j -->
        <statement statement-id="ac-2_smt.k"><!-- cut --></statement>
    </implemented-requirement>
</control-implementation>
```

5.4.3. Organization: Single Statement

If there are no lettered parts in the control definition, such as with AC-2 (1), there must be exactly one `statement` assembly.

Single-Statement Representation

```
<!-- system-implementation -->
<control-implementation>
    <!-- cut -->
    <implemented-requirement control-id="ac-2.1">
        <statement statement-id="ac-2.1_smt"><!-- cut --></statement>
    </implemented-requirement>
</control-implementation>
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization	

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

5.4.4. Response: Overview

Within each `statement` assembly, all responses must be provided within one or more `by-component` assemblies. There must always be a component defined in the `system-implementation` representing the system as a whole (**"THIS SYSTEM"**), even if individual components are defined that comprise the system.

See *Appendix A, Working with Components* for more information.

An OSCAL-based FedRAMP SSP should define individual components of the system. Components are not just hardware and software. Policies, processes, FIPS 140 validation information, interconnections, services, and underlying systems (leveraged authorizations) are all components.

With OSCAL, the content in the cell next to *Part a* must be broken down into its individual components and responded to separately

COMPONENT APPROACH: AC-2 What is the solution and how is it implemented?

Part a

Component	Description
THIS SYSTEM	Describes how *part a* is satisfied holistically, or where the description does not fit with a defined component.
Platform	Describes how *part a* is satisfied by the platform.
Web-server	Describes how *part a* is satisfied by the web server
Process	Describes how *part a* is satisfied by an identified process within this organization.
Inherited	Describes what is inherited from the underlying Infrastructure as a Service (IaaS) provider to satisfy *part a*.

Part b

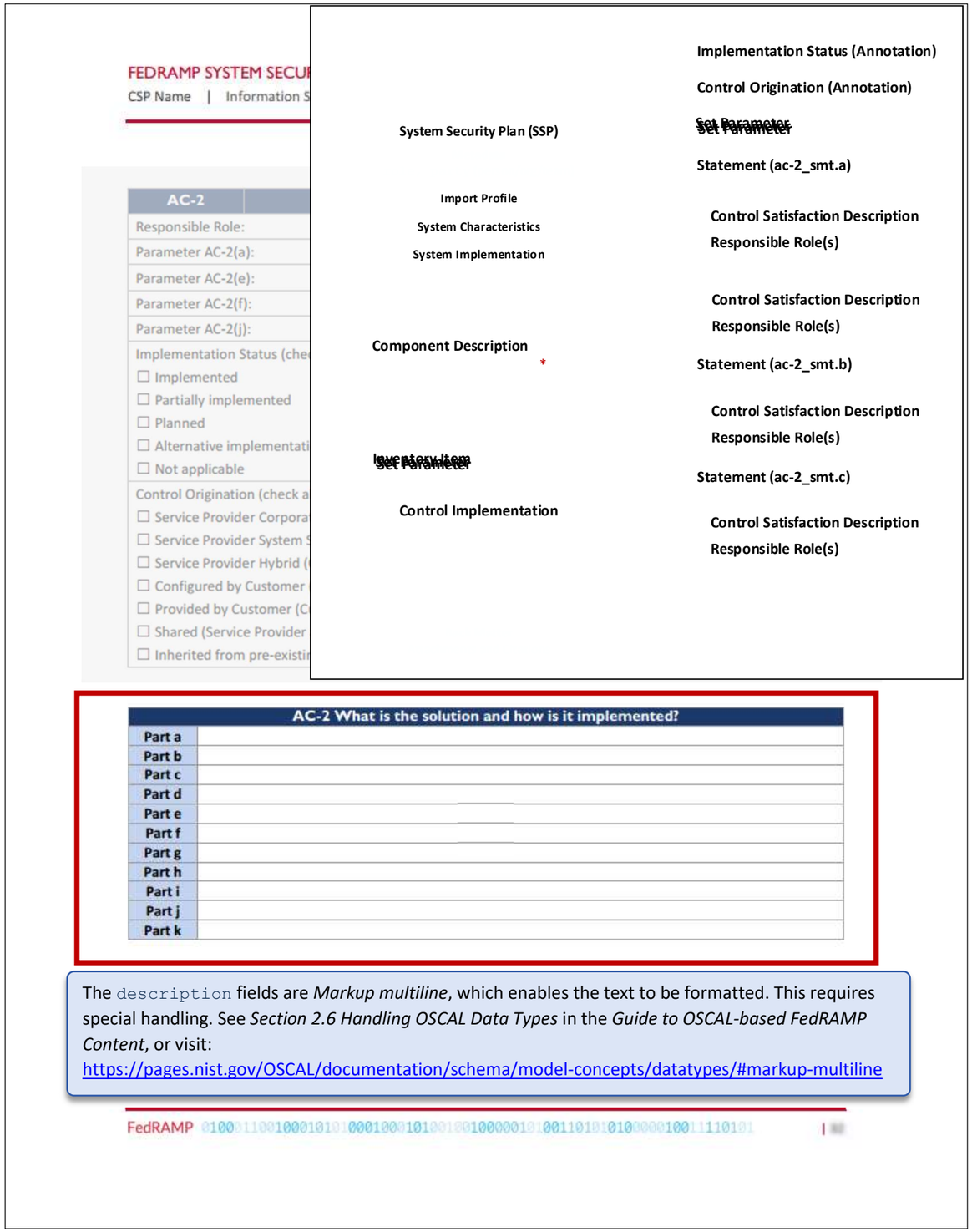
Component	Description
THIS SYSTEM	Describes how *part b* is satisfied holistically, or where the description does not fit with a defined component.
Platform	Describes how *part b* is satisfied by the platform.
Web-server	Describes how *part b* is satisfied by the web server
Process	Describes how *part b* is satisfied by an identified process within this organization.
Inherited	Describes what is inherited from the underlying Infrastructure as a Service (IaaS) provider to satisfy *part b*.

The following pages provide examples.

Converting Legacy SSPs to OSCAL

For CSPs converting their existing MS Word-based SSP to OSCAL, FedRAMP allows the entire part response to initially be associated with the **"THIS SYSTEM"** component. Once converted, the CSP is encouraged to begin defining individual components and move content from the general **"THIS SYSTEM"**" description to the component-specific description.

See *Appendix B, Converting a Legacy SSP to* OSCAL for an alternative OSCAL control representation, which aligns better with legacy SSP content.



AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

The `description` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

5.4.5. Response: Example

Within each of the `statement` assemblies, all responses appear in one or more `by-component` assemblies. Each `by-component` assembly references a `component` defined in the `system-implementation` assembly.

Representation

```
<system-implementation>
    <!-- leveraged-authorization, user -->
    <component uuid="uuid-value" type="software">
        <title>Component Title</title>
        <description>
            <p>Description of the component.</p>
        </description>
        <status state="operational"/>
    </component>

    <component uuid="uuid-value" type="process">
        <title>Process Title</title>
        <description>
            <p>Description of the component.</p>
        </description>
        <status state="operational"/>
        <responsible-role role-id="admin-unix">
            <party-uuid>3360e343-9860-4bda-9dfc-ff427c3dfab6</party-uuid>
        </responsible-role>
    </component>
</system-implementation>

<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">

            <by-component uuid="uuid-value" component-uuid="uuid-of-software-component">
                <description>
                    <p>Describe how is the software component satisfying the control.</p>
                </description>
            </by-component>
            <by-component uuid="uuid-value" component-uuid="uuid-of-process-component">
                <description>
                    <p>Describe how is the process satisfies the control.</p>
                </description>
            </by-component>
            <!-- repeat by-component assembly for each component related to part a. -->

        </statement>
        <!-- repeat statement assembly for statement part (b, c, etc.) as needed. -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

See Section 5.4.10, XPath Queries for Control Implementation Descriptions

NOTES:

- All `statement-id` values must be cited as they appear in the NIST SP 800-53, Revision 4 or Revision 5 OSCAL catalogs: https://github.com/usnistgov/oscal-content/tree/master/nist.gov/SP800-53

When converting a legacy SSP to OSCAL, the legacy content can be associated with the "This System"" component until the SSP author is able to provide more granular content.

13.1. Access Control (AC)

AC-1 Access Control Policy and Procedures Requirements (H)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and
(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1	Control Summary Information
Responsible Role:	
Parameter AC-1(a):	
Parameter AC-1(b)(1):	
Parameter AC-1(b)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

AC-1 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

5.4.6. Response: "This System" Component

There must always be a **"This System"** component in the SSP. This is used in several ways:

- **Holistic Overview**: If the SSP author wishes to provide a more holistic overview of how several components work together, even if details are provided individually in other `by-component` assemblies.
- **Catch-all**: Any control response that does not cleanly align with another system component may be described in the the **"This System"** component.
- **Legacy SSP Conversion**: When converting a legacy SSP to OSCAL, the legacy control response statements may initially be associated with the **"This System"** component until the SSP author is able to provide responses for individual components.

Representation

```
<system-implementation>
    <!-- leveraged-authorization, user -->
    <component uuid="uuid-value" type="this-system">
        <title>This System</title>
        <description>
            <p>Description of the component.</p>
        </description>
        <status state="operational"/>
    </component>
</system-implementation>

<control-implementation>
    <!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">

            <by-component uuid="uuid-value" component-uuid="uuid-of-this-system-component">
                <description>
                    <p>Describe how individual components are working together.</p>
                    <p>Describe how the system - as a whole - is satisfying this
statement.</p>
                    <p>This can include policy, procedures, hardware, software, etc.</p>
                </description>
            </by-component>

        </statement>
        <!-- repeat statement assembly for statement part (b, c, etc.) as needed. -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

XPath Queries

See Section 5.4.10, XPath Queries for Control Implementation Descriptions

NOTES:

- Although the name of the component is **"This System"**, non-technical solutions may also be discussed here, such as policies and procedures.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

13.1. Access Control (AC)

AC-1 Access Control Policy and Procedures Requirements (H)

The organization:

(a) Develops, documents, and disseminates to [*Assignment: organization-defined personnel or roles*]:

(1) An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

(2) Procedures to facilitate the implementation of the access control policy and associated access controls; and

(b) Reviews and updates the current:

(1) Access control policy [*FedRAMP Assignment: at least annually*]; and

(2) Access control procedures [*FedRAMP Assignment: at least annually or whenever a significant change occurs*].

AC-1	Control Summary Information
Responsible Role:	
Parameter AC-1(a):	
Parameter AC-1(b)(1):	
Parameter AC-1(b)(2):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific)	

AC-1 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

5.4.7. Linking to Artifacts

Any time policies, procedures, plans, and similar documentation are cited in a control response, they must be linked.

For the legacy approach, when responding within the by-component assembly for **"this system"**, the link must be within the same by-component assembly where the artifact is cited.

Representation: Legacy Approach Example - No Policy Component

```
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <statement uuid="uuid-value" statement-id="ac-1_smt.a">
            <by-component component-uuid="uuid-of-this-system" uuid="uuid-value">
                <description>
                    <p>Describe how Part a is satisfied within the system.</p>
                </description>
                <link href="#uuid-of-policy-resource-in-back-matter" rel="policy" />
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

For the component approach, use the component representing the policy. The link should be in the component, but may be added directly to the by-component as well.

Representation: Component Approach Example

```
<system-implementation>
    <!-- leveraged-authorization, user -->
    <component uuid="uuid-value" type="policy">
        <title>Access Control and Identity Management Policy</title>
        <description>
            <p>An example component representing a policy.</p>
        </description>
        <link href="#uuid-of-policy-resource-in-back-matter" rel="policy" />
        <status state="operational"/>
    </component>
</system-implementation>
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-1">
        <statement uuid="uuid-value" statement-id="ac-1_smt.a">
            <by-component component-uuid="uuid-of-policy-component" uuid="uuid-value">
                <description>
                    <p>Describe how this policy satisfies Part a.</p>
                </description>
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

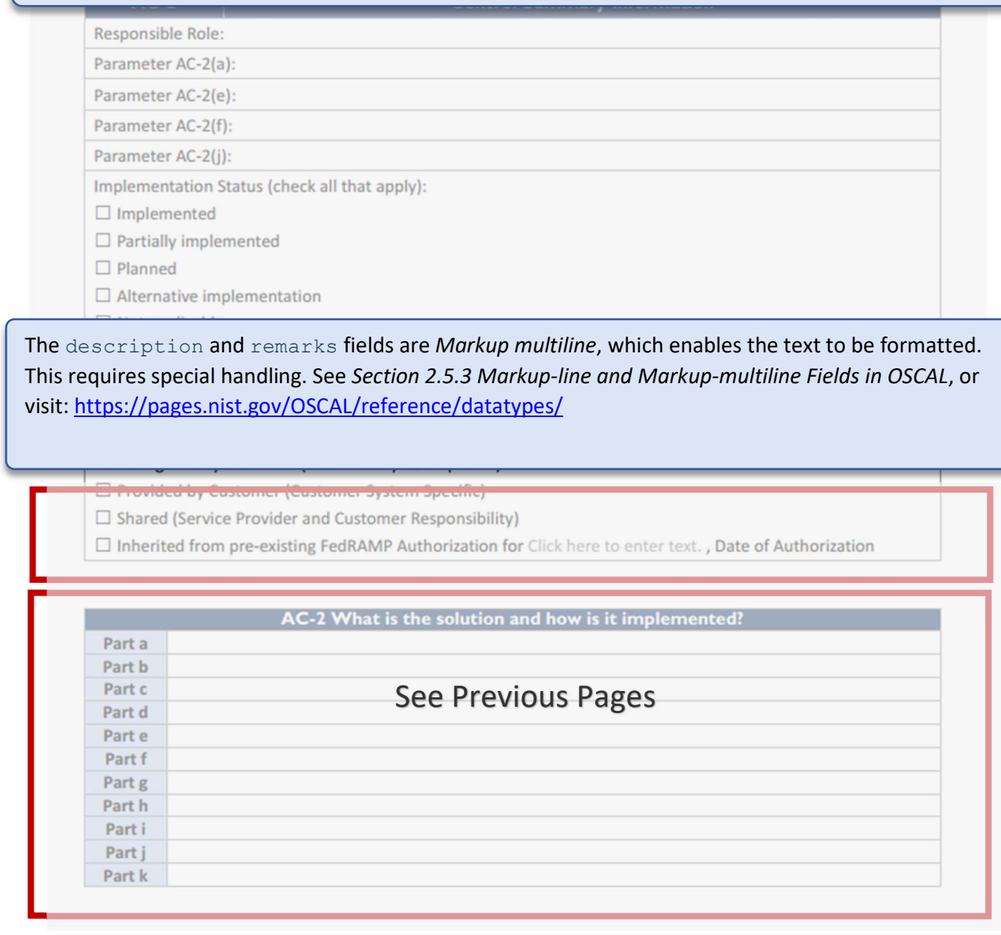
For either example above, the policy must be present as a `resource` in `back-matter`.

In Back Matter

```
<back-matter>
    <resource uuid="uuid-value">
        <title>Access Control and Identity Management Policy</title>
        <rlink media-type="application/pdf" href="./documents/policies/sample_policy.pdf" />
        <base64 filename="sample_policy.pdf" media-type="application/pdf">00000000</base64>
    </resource>
</back-matter>
```

When a responsibility is linked to a provided assembly it indicates to a leveraging system that if inheritance is desired, the customer responsibility must be satisfied. If the leveraging system elects to ignore inheritance and implement their own solution, the linked responsibility may be ignored.

If a responsibility is always required, add it to the by-component assembly representing **"this system"** and do not link it to a provided assembly.



The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/reference/datatypes/

A `role` and associated `party` should be identified in the leveraged system's metadata identifying who leveraging customers should contact regarding inherited capabilities. The role should be supplied in the `responsible-role` field of the `provided` assembly.

A `role` with an `id="customer"` must be defined in the `metadata`, and referenced by the `responsible-role` field of the `responsibility` assembly.

5.4.8. Response: Identifying Inheritable Controls and Customer Responsibilities

For systems that may be leveraged, OSCAL enables a robust mechanism for providing both inheritance details as well as customer responsibilities (referred to as consumer responsibilities by NIST). OSCAL is designed to enable leveraged and leveraging system SSP details to be linked by tools for validation.

Within the appropriate `by-component` assembly, include an `export` assembly. Use `provided` to identify a capability that may be inherited by a leveraging system. Use `responsibility` to identify a customer responsibility. If a responsibility must be satisfied to achieve inheritance, add the `provided-uuid` flag to the `responsibility` field.

Representation

```
<!-- system-implementation -->
<control-implementation><!-- cut -->
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">
            <by-component uuid="uuid-value" component-uuid="uuid-of-this-system-component">
                <description>
                    <p>Describe how the system - as a whole - is satisfying this
statement.</p>
                </description>
                <export>
                    <responsibility uuid="uuid-value">
                        <description>
                            <p>Leveraging system's responsibilities in satisfaction of AC-
2.</p>
                            <p>Not linked to inheritance, so this is always required.</p>
                        </description>
                        <responsible-role role-id="customer" />
                    </responsibility>
                </export>
            </by-component>
            <by-component uuid="uuid-value" component-uuid="uuid-of-software-component">
                <description>
                    <p>Describe how the software is satisfying this statement.</p>
                </description>
                <export>
                    <provided uuid="uuid-value">
                        <description>
                            <p>Customer appropriate description of what may be inherited.</p>
                        </description>
                        <responsible-role role-id="poc-for-customers" />
                    </provided>

                    <responsibility uuid="uuid-value" provided-uuid="uuid-of-provided">
                        <description>
                            <p>Customer responsibilities if inheriting this capability.</p>
                        </description>
                        <responsible-role role-id="customer" />
                    </responsibility>
                </export>
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
```

See Section 5.4.10, XPath Queries for Control Implementation Descriptions

See the NIST OSCAL Leveraged Authorization Presentation for more information.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

The `provided-uuid` flag in `inherited` links to the provided statement in the leveraged system's SSP.

The `responsibility-uuid` flag in satisfied links to the `responsibility` statement in the leveraged system's SSP.

Both may be exposed to the leveraging system via the OSCAL Inheritance and Responsibility model when the leveraging system owner is not entitled to see the leveraged system's SSP as is typical with FedRAMP-authorized systems. This model replaces the CRM.

NOTE: At time of publication, NIST estimates this model will be released during the Summer of 2021. Along with the model, NIST intends to release a capability allowing CSPs to generate the Inheritance and Responsibility file automatically from its SSP.

Control Origination (check all that apply):

- ☐ Service Provider Corporate
- ☐ Service Provider System Specific
- ☐ Service Provider Hybrid (Corporate and System Specific)
- ☐ Configured by Customer (Customer System Specific)
- ☐ Provided by Customer (Customer System Specific)
- ☐ Shared (Service Provider and Customer Responsibility)
- ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text. , Date of Authorization

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

The `description` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.5.3 Markup-line and Markup-multiline Fields in OSCAL*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

5.4.9. Leveraged Authorization Response: Inheriting Controls, Satisfying Responsibilities

When the current system is inheriting a control from or meeting customer responsibilities defined by an underlying authorization , the leveraged system must first be defined as described in *Section 4.15, Leveraged Authorizations* before it may be referenced in a control response. The `by-component` assembly references these components.

IMPORTANT: The leveraged system may provide a single component representing the entire leveraged system, or may provide individual system components as well. In either case, the `inherited-uuid` property in the component when defined in the leveraging system's SSP. This is the

Representation

```
<system-implementation>
    <component uuid="uuid-value" type="this-system"><!-- cut --></component>
    <component uuid="uuid-value" type="leveraged-system">
        <title><b>LEVERAGED SYSTEM as a whole (IaaS)</b></title>
        <prop name="leveraged-authorization-uuid" value="uuid-of-LA-in-this-SSP" />
        <prop name="inherited-uuid" value="uuid-of-component-in-leveraged-SSP" />
    </component>
    <component uuid="uuid-value" type="service">
        <title>Service Provided by Leveraged System</title>
        <prop name="leveraged-authorization-uuid" value="uuid-of-LA-in-this-SSP" />
        <prop name="inherited-uuid" value="uuid-of-component-in-leveraged-SSP" />
    </component>
</system-implementation>
<control-implementation>
    <implemented-requirement uuid="uuid-value" control-id="ac-2">
        <statement uuid="uuid-value" statement-id="ac-2_smt.a">
            <by-component uuid="uuid-value" component-uuid="uuid-of-this-system-component">
                <description><p>Describe what is satisfied by this system.</p></description>
            </by-component>

            <by-component uuid="uuid-value" component-uuid="uuid-leveraged-system-component">
                <description>
                    <p>Describe what is inherited from the leveraged system in satisfaction
                        of this control statement.</p>
                </description>

                <inherited provided-uuid="uuid-of-provided" uuid="uuid-value">
                    <description>
                        <p>Optional: Information provided by leveraged system.</p>
                    </description>
                </inherited>

                <satisfied responsibility-uuid="uuid-of-responsibility" uuid="uuid-value" >
                    <description>
                        <p>Description of how the responsibility was satisfied.</p>
                    </description>
                </satisfied>
            </by-component>
        </statement>
        <!-- repeat statement assembly for statement part (b, c, etc.) as needed. -->
    </implemented-requirement>
</control-implementation>
<!-- back-matter -->
```

See Section 5.4.10, XPath Queries for Control Implementation Descriptions

See the NIST OSCAL Leveraged Authorization Presentation for more information.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

AC-2	Control Summary Information
Responsible Role:	
Parameter AC-2(a):	
Parameter AC-2(e):	
Parameter AC-2(f):	
Parameter AC-2(j):	
Implementation Status (check all that apply): ☐ Implemented ☐ Partially implemented ☐ Planned ☐ Alternative implementation ☐ Not applicable	See Previous Pages
Control Origination (check all that apply): ☐ Service Provider Corporate ☐ Service Provider System Specific ☐ Service Provider Hybrid (Corporate and System Specific) ☐ Configured by Customer (Customer System Specific) ☐ Provided by Customer (Customer System Specific) ☐ Shared (Service Provider and Customer Responsibility) ☐ Inherited from pre-existing FedRAMP Authorization for Click here to enter text., Date of Authorization	

AC-2 What is the solution and how is it implemented?	
Part a	
Part b	
Part c	
Part d	
Part e	
Part f	
Part g	
Part h	
Part i	
Part j	
Part k	

5.4.10. XPath Queries for Control Implementation Descriptions

Use the following XPath queries to retrieve basic control response information. For any given control response part, tools should list the name of each component cited by a `by-component` assembly, as well as the description.

XPath Queries

```
Number of cited components for AC-2, part a (Integer):
  count(/*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-component)

Name of first component related to AC-2, part a:
  /*/system-implementation/component[@uuid=/*/control-implementation/implemented-
  requirement[@control-id="ac-2"]/statement[@statement-id="ac-2_smt.a"]/by-
  component[1]/@component-uuid]/title

"What is the solution and how is it implemented?" for AC-2, Part (a), first component:
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-component[1]/description/node()

Is there a customer responsibility for the first component in AC-2, part a?
  (true/false):
  boolean(/*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-component[1]
  /prop[@name='responsibility'][@value='customer'])

Customer responsibility statement for the first component in AC-2, part a:
  /*/control-implementation/implemented-requirement[@control-id="ac-
  2"]/statement[@statement-id="ac-2_smt.a"]/by-
  component[1]/prop[@name='responsibility'][@value='customer']/remarks/node()
```

NOTES:

- Replace "ac-2" with target control-id.
- Replace "ac-2_smt.a" with target control statement-id.
- Replace "[1]" with "[2]", "[3]", etc. as needed to reference is by-component statement.

15. ATTACHMENTS

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. ***Example*** Enter Information System Abbreviation ***A1 ISPP xx v1.0***. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Names of Provided Attachments

Attachment	File Name	File Extension
Information Security Policies and Procedures	Enter Information System Abbreviation A1 ISPP xx v1.0	. enter extension
User Guide	Enter Information System Abbreviation A2 UG v1.0	. enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA (if needed)	Enter Information System Abbreviation A4 PIA v1.0	. enter extension
Rules of Behavior	Enter Information System Abbreviation A5 ROB v1.0	. enter extension
Information System Contingency Plan	Enter Information System Abbreviation A6 ISCP v1.0	. enter extension
Configuration Management Plan	Enter Information System Abbreviation A7 CMP v1.0	. enter extension
Incident Response Plan	Enter Information System Abbreviation A8 IRP v1.0	. enter extension
CIS Workbook	Enter Information System Abbreviation A9 CIS Workbook v1.0	. enter extension
FIPS 199	Included in Section 15	
Inventory	Enter Information System Abbreviation A13 INV v1.0	. enter extension

6. ATTACHMENTS

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The resource's `title` and `description` must be used to provide a human-readable indicator of what attachment is being referenced, however, OSCAL extensions must also be provided when applicable for machine readability. The following table describes how each attachment is handled:

ATTACHMENT	MACHINE READABLE	HOW TO HANDLE
Policies and Procedures	No	Attach using the `back-matter`, `resource` syntax. For Policies, `resource` must include a `prop` with `@name="type"` and `@value="policy"`. For Procedures, `resource` must include a `prop` with `@name="type"` and `@value="procedure"`.
User Guide	No	Attach using the `back-matter`, `resource` syntax. For User Guides, `resource` must include a `prop` with `@name="type"` and `@value="guide"`.
Digital Identity Worksheet	Yes	Incorporated above. See the *Digital Identity Determination* Section.
Privacy Threshold Analysis (PTA)	Yes	Incorporated into System Information. See the *Privacy Impact Assessment* Section.
Privacy Impact Assessment (PIA)	No (Future)	Attach using the `back-matter`, `resource` syntax. For PIA, `resource` must include a `prop` with `@name="type"` and `@value= value="privacy-impact-assessment".`
Rules of Behavior	No	Attach using the `back-matter`, `resource` syntax. For PIA, `resource` must include a prop with `@name="type"` and `@value= value="rules-of-behavior".`
Information System Contingency Plan	No	Attach using the `back-matter`, `resource` syntax. For PIA, `resource` must include a prop with `@name="type"` and `@value= value="rules-of-behavior".`
Configuration Management Plan	No	Attach using the `back-matter`, `resource` syntax. For PIA, `resource` must include a prop with `@name="type"` and `@value= value="plan".`
Incident Response Plan	No	Attach using the `back-matter`, `resource` syntax. For PIA, `resource` must include a prop with `@name="type"` and `@value= value="plan".`
CIS Workbook	Yes	This can be generated from the content in the Security Controls section and no longer needs to be maintained separately or attached.
FIPS-199	Yes	Incorporated above. See the *Security Objectives Categorization (FIPS-199)* Section.

Inventory	Yes	See the *System Inventory* Section below.

FEDRAMP SYSTEM SECURITY PLAN (SSP) _____ BASELINE TEMPLATE

CSP Name | Information System Name *Version #.#, Date*

15. ATTACHMENTS

A recommended attachment file naming convention is <information system abbreviation> <attachment number> <document abbreviation> <version number> (for example, "Information System Abbreviation A8 IRP v1.0"). Use this convention to generate names for the attachments. Enter the appropriate file names and file extensions in Table 15-1 to describe the attachments provided. Make only the following additions/changes to Table 15-1:

- The first item, Information Security Policies and Procedures (ISPP), may be fulfilled by multiple documents. If that is the case, add lines to Table 15-1. to differentiate between them using the "xx" portion of the File Name. ***Example*** Enter Information System Abbreviation ***A1 ISPP xx v1.0***. Delete the "xx" if there is only one document.
- Enter the file extension for each attachment.
- Do not change the Version Number in the File Name in Table 15-1. . (Information System Abbreviation, attachment number, document abbreviation, version number)

Table 15-1. Names of Provided Attachments

Attachment	File Name	File Extension
Information Security Policies and Procedures	Enter Information System Abbreviation A1 ISPP xx v1.0	. enter extension
User Guide	Enter Information System Abbreviation A2 UG v1.0	. enter extension
Digital Identity Worksheet	Included in Section 15	
PTA	Included in Section 15	
PIA (if needed)	Enter Information System Abbreviation A4 PIA v1.0	. enter extension
Rules of Behavior	Enter Information System Abbreviation A5 ROB v1.0	. enter extension
Information System Contingency Plan	Enter Information System Abbreviation A6 ISCP v1.0	. enter extension
Configuration Management Plan	Enter Information System Abbreviation A7 CMP v1.0	. enter extension
Incident Response Plan	Enter Information System Abbreviation A8 IRP v1.0	. enter extension
CIS Workbook	Enter Information System Abbreviation A9 CIS Workbook v1.0	. enter extension
FIPS 199	Included in Section 15	
Inventory	Enter Information System Abbreviation A13 INV v1.0	. enter extension

6.1. Attachments

Classic FedRAMP attachments include a mix of items. Some lend well to machine-readable format, while others do not. Machine-readable content is typically addressed within the OSCAL-based FedRAMP SSP syntax, while policies, procedures, plans, guidance, and the rules of behavior documents are all treated as classic attachments, as described in the *Citations, Attachments, and Embedded Content in OSCAL Files* Section. The following table describes how each attachment is handled:

Attachment Representation

```
<!-- cut -->
<back-matter>
    <resource uuid="uuid-value">
        <desc>Policy document</desc>
        <prop name="type" ns="https://fedramp.gov/ns/oscal" value="policy"/>
        <prop name="title" ns="https://fedramp.gov/ns/oscal" value="Document Title"/>
        <prop name="publication" ns="https://fedramp.gov/ns/oscal" value="2021-01-01Z"/>
        <prop name="version" ns="https://fedramp.gov/ns/oscal" value="1.2"/>
        <!-- Add rlink with relative path or embed with base64 encoding -->
        <base64>00000000</base64>
    </resource>
    <resource uuid="uuid-value" />
    <!-- cut: policies 3 - 13 -->
    <resource uuid="uuid-value" />
    <resource uuid="uuid-value" />
    <!-- cut: procedure 2 - 13 -->
</back-matter>
```

FedRAMP Extensions & Accepted Values

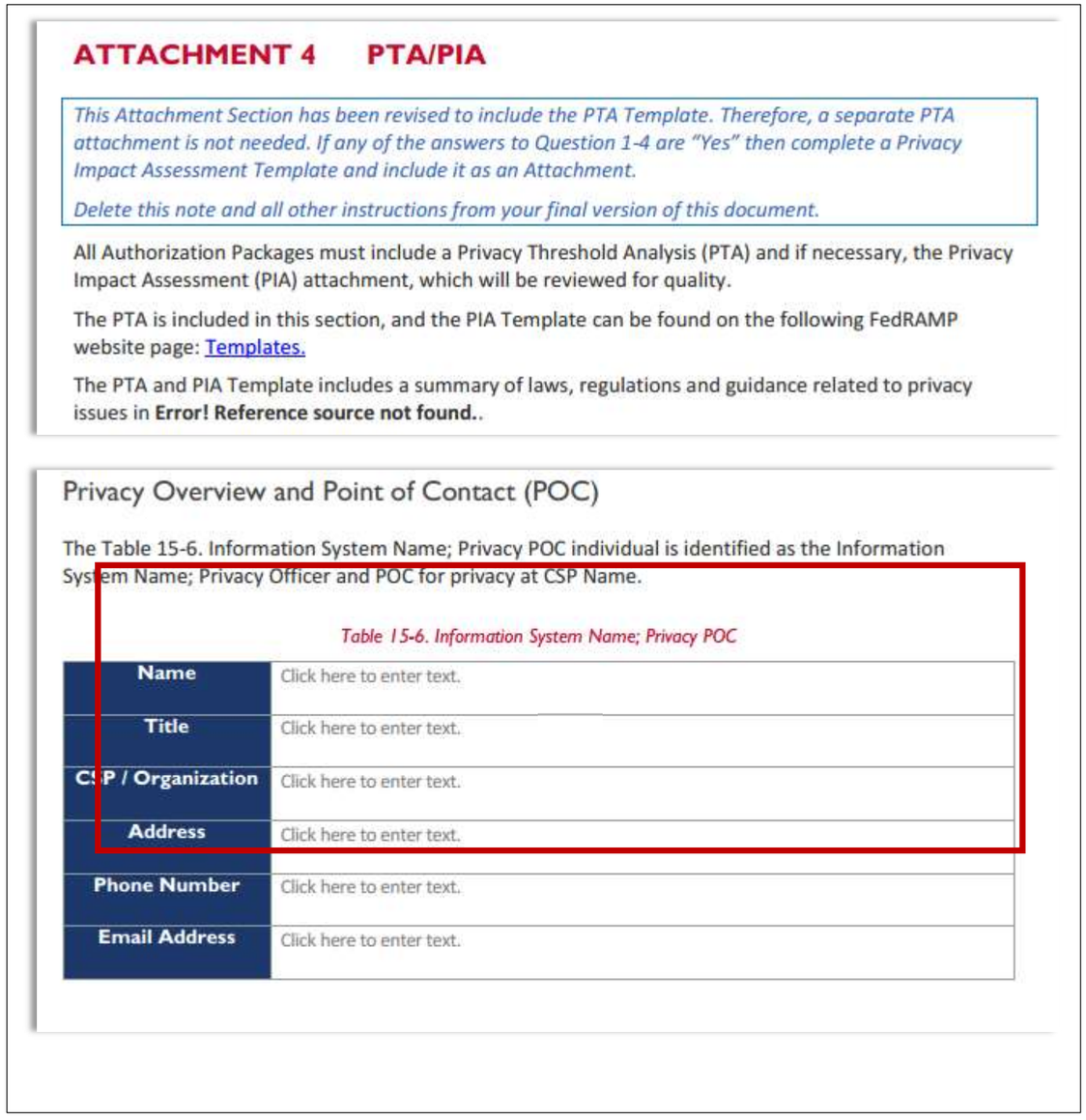
prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="type"`
  - **Valid**: policy, procedure, guide, pia, rob, plan
- `name="title"`
- `name="publication"`
- `name="version"`

XPath Queries

```
The Number of Policies Attached:
  count(/*/back-matter/resource/prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][string(./@value)="policy"])

Attachment (Embedded Base64 encoded):
  /*/back-matter/resource[@id="att-policy-1"]/base64
  OR (Relative Link):
  /*/back-matter/resource[@id="att-policy-1"]/rlink/@href

Title of First Policy Document:
  /*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [string(.)="policy"][1]/../prop[@name="title"][@ns="https://fedramp.gov/ns/oscal"]
```

Replace "policy" with "plan", "rob", etc. for each attachment type.



ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

Privacy Overview and Point of Contact (POC)

The Table 15-6. Information System Name; Privacy POC individual is identified as the Information System Name; Privacy Officer and POC for privacy at CSP Name.

Table 15-6. Information System Name; Privacy POC

Name	Click here to enter text.
Title	Click here to enter text.
CSP / Organization	Click here to enter text.
Address	Click here to enter text.
Phone Number	Click here to enter text.
Email Address	Click here to enter text.

6.2. Privacy Impact Assessment: POC

Much of the Privacy Impact Assessment (PIA) is absorbed into constructs addressed earlier in this document. The Privacy POC is handled the same as other roles. The same is true for the laws and regulations. A role with an ID value of "`privacy-poc`" is required. Use the `responsible-party` assembly to associate this role with the party assembly containing the Privacy Officer's information.

Attachment Representation

```
<!-- cut -->
<metadata>
    <role id="privacy-poc">
        <title>Privacy Official's Point of Contact</title>
        <desc>The individual responsible for the PTA and if necessary the PIA.</desc>
    </role>
    <party uuid="uuid-of-csp" type="organization">
        <name>Cloud Service Provider (CSP) Name</name>
    </party>
    <party uuid="uuid-of-person-7">
        <person>
            <name>[SAMPLE]Person Name 7</name>
            <prop name="job-title" value="Individual's Title"/>
            <address>
                <addr-line>Suite 0000</addr-line>
                <addr-line>1234 Some Street</addr-line>
                <city>Haven</city>
                <state>ME</state>
                <postal-code>00000</postal-code>
            </address>
            <email-address>name@org.domain</email-address>
            <telephone-number>000-000-0000</telephone-number>
            <member-of-organization>uuid-of-csp</member-of-organization>
        </person>
    </party>
    <!-- cut -->
    <responsible-party role-id="privacy-poc">
        <party-uuid>uuid-of-person-7</party-uuid>
    </responsible-party>
</metadata>
```

NIST-Defined Identifier
Required Role ID:
- `privacy-poc`

XPath Queries

Privacy POC Name:
```
/*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="privacy-poc"]/party-uuid]]/name
```

NOTE: Replace "name" with "email-address" or "telephone-number" above as needed.

Privacy POC's Address:
```
/*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="privacy-poc"]/party-uuid]]/address/addr-line
```

NOTE: Replace "addr-line" with "city", "state", or "postal-code" above as needed.

Privacy POC's Title:
```
/*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="privacy-poc"]/party-uuid]]/prop[@name='title'][@ns='https://fedramp.gov/ns/oscal']
```

Company/Organization:
```
/*/metadata/party[@uuid=/*/metadata/party[@uuid=[/*/metadata/responsible-party[@role-id="privacy-poc"]/party-uuid]]/member-of-organization]/name
```

ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

Table 15-7. <Information System Name> Laws and Regulations

Identification Number	Title	Date	Link
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

6.3. Privacy Impact Assessment: Laws and Regulations

Much of the PIA is absorbed into constructs addressed earlier in this document. The Privacy POC is handled the same as other roles. The same is true for the laws and regulations.

Attachment Representation

```
<!-- cut -->
<back-matter>
    <resource uuid="uuid-value">
        <title>[SAMPLE]Privacy-Related Law Citation</title>
        <prop name="type" ns="https://fedramp.gov/ns/oscal" value="law" />
        <prop name="type" ns="https://fedramp.gov/ns/oscal" value="pii" />
        <document-id scheme="https://www.doi.org/" value="Identification Number" />
        <prop name="publication" ns="https://fedramp.gov/ns/oscal" value="Publication" />
        <rlink href="https://domain.example/path/to/document.pdf" />
    </resource>
</back-matter>
```

XPath Queries

```
Number of Privacy Laws and Regulations:
  count((/*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [(string(.)="law" or (string(.)="regulation")])/../prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii")])

Privacy Laws and Regulations - Identification Number:
  ((/*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [(string(.) = "law") or (string(.)="regulation")])/../prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii")])[1]/../document-id

Laws and Regulations - Title:
  ((/*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [(string(.) = "law") or (string(.)="regulation")])/../prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii")])[1]/../title

Privacy Laws and Regulations - Date:
  ((/*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [(string(.) = "law") or (string(.)="regulation")])/../prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii")])[1]/../
  prop[@name="publication"][@ns="https://fedramp.gov/ns/oscal"]

Privacy Laws and Regulations - Link:
  ((/*/back-matter/resource/prop[@name="type"][@ns="https://fedramp.gov/ns/oscal"]
  [(string(.) = "law") or (string(.)="regulation")])/../prop[@name="type"]
  [@ns="https://fedramp.gov/ns/oscal"][(string(.) = "pii")])[1]/../rlink/@href
```

Replace "[1]" with "[2]", "[3]", etc.

ATTACHMENT 4 PTA/PIA

This Attachment Section has been revised to include the PTA Template. Therefore, a separate PTA attachment is not needed. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment Template and include it as an Attachment.

Delete this note and all other instructions from your final version of this document.

All Authorization Packages must include a Privacy Threshold Analysis (PTA) and if necessary, the Privacy Impact Assessment (PIA) attachment, which will be reviewed for quality.

The PTA is included in this section, and the PIA Template can be found on the following FedRAMP website page: Templates.

The PTA and PIA Template includes a summary of laws, regulations and guidance related to privacy issues in **Error! Reference source not found.**.

DESIGNATION

Check one.

☐ A Privacy Sensitive System

☐ Not a Privacy Sensitive System (in its current version)

The Privacy Impact Assessment Template can be found on the following FedRAMP website page: Templates.

QUALIFYING QUESTIONS

Select One	1.	Does the ISA collect, maintain, or share PII in any identifiable form?
Select One	2.	Does the ISA collect, maintain, or share PII information from or about the public?
Select One	3.	Has a Privacy Impact Assessment ever been performed for the ISA?
Select One	4.	Is there a Privacy Act System of Records Notice (SORN) for this ISA system? If yes; the SORN identifier and name is: Enter SORN ID/Name.

If answers to Questions 1-4 are all "No" then a Privacy Impact Assessment may be omitted. If any of the answers to Question 1-4 are "Yes" then complete a Privacy Impact Assessment.

6.4. Privacy Impact Assessment: Designation and Qualifying Questions

Attachment Representation

```
<!-- cut -->
<system-characteristics>
    <system-information>
        <!-- Attachment 4, PTA/PIA Designation -->
        <prop name="privacy-sensitive" value="yes"/>
        <!--Does the ISA collect, maintain, or share PII in any identifiable form? -->
        <prop name="pta-1" class="pta" ns="https://fedramp.gov/ns/oscal" value="yes"/>
        <!--Does the ISA collect, maintain, share PII info from or about the public? -->
        <prop name="pta-2" class="pta" ns="https://fedramp.gov/ns/oscal" value="yes"/>
        <!--Has a Privacy Impact Assessment ever been performed for the ISA? -->
        <prop name="pta-3" class="pta" ns="https://fedramp.gov/ns/oscal" value="yes"/>
        <!--Is there a Privacy Act System of Records Notice (SORN) for this ISA system? -->
        <prop name="pta-4" class="pta" ns="https://fedramp.gov/ns/oscal">yes</prop>
        <prop name="sorn-id" class="pta" ns="https://fedramp.gov/ns/oscal" value="SORNID1"/>
        <!-- information-type -->
    </system-information>
</system-characteristics>
```

FedRAMP Extensions & Accepted Values

prop (`ns="https://fedramp.gov/ns/oscal", class="pta"`):

- `name="privacy-sensitive"`
  - **Valid:** yes, no
- `name="pta-1"`
  - **Valid:** yes, no
- `name="pta-2"`
  - **Valid:** yes, no
- `name="pta-3"`
  - **Valid:** yes, no
- `name="pta-4"`
  - **Valid:** yes, no

XPath Queries

```
Privacy Designation (yes = Privacy Sensitive):
  /*/system-characteristics/system-information/prop[@name="privacy-sensitive"]/@value

Qualifying Question #1:
  /*/system-characteristics/system-information/prop[@name="pta-1"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Qualifying Question #2:
  /*/system-characteristics/system-information/prop[@name="pta-2"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Qualifying Question #3:
  /*/system-characteristics/system-information/prop[@name="pta-3"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Qualifying Question #4:
  /*/system-characteristics/system-information/prop[@name="pta-4"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value

Qualifying Question #4:
  /*/system-characteristics/system-information/prop[@name="sorn-id"]
  [@ns="https://fedramp.gov/ns/oscal"]/@value
```

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for qua

When completed, FedRAMP will accept this inventory workbook as the inventory informat by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page

Note: A complete and detailed list of the system hardware and software inventory is requi SP 800-53, Rev 4 CM-8.

NOTE: OSCAL also uses components to represent content that does not typically appear in the system inventory. When rendering a presentation of system inventory, tools should offer users the option to exclude components such as Interconnections, services, policies, procedures, the system (as a whole), leveraged systems (as a whole), and FIPS 140 validation details.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

Software and Database Inventories				Any Inventory				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Acme Software	Acme CloudApp v1.0		CRM					
Oracle	Oracle v11		Records Management					

6.5. System Inventory Approach

OSCAL makes two approaches available for depicting the system inventory:

- **Flat-File Approach**: Similar to today's FedRAMP Integrated inventory workbook, where all of the information on a spreadsheet row is captured in a single assembly.
- **Component-Based Approach**: A component is defined once with as much known detail as possible, and inventory-items point to components for common information.

FedRAMP prefers the component-based approach, accepts the flat-file approach to aid CSPs who are converting their existing MS-Excel based FedRAMP Integrated Inventory Workbook to OSCAL. **FedRAMP SSP tools must support both approaches.**

Type: "software"
Name: "Database Product"
Vendor: "Vendor Name"
Version: "1.2.3"
IPv4: 1.1.1.30

Type: "software"
Name: "Database Product"
Vendor: "Vendor Name"
Version: "1.2.3"
IPv4: 2.1.1.30

Type: "software"
Name: "Web Server Product"
Vendor: "Vendor Name"
Version: "4.3.2"
IPv4: 1.1.1.20

Type: "software"
Name: "Web Server Product"
Vendor: "Vendor Name"
Version: "4.3.2"
IPv4: 2.1.1.20

Type: "software"
Name: "Operating System Product"
Vendor: "Vendor Name"
Version: "8.4.1"
IPv4: 1.1.1.20

Type: "software"
Name: "Operating System Product"
Vendor: "Vendor Name"
Version: "8.4.1"
IPv4: 2.1.1.20

Flat-File Inventory Approach

With the **flat-file approach**, all content on a spreadsheet row appears in a single OSCAL `inventory-item` assembly. This results in a great deal of redundant information but is a simple transition from the current spreadsheet approach.

With the **component-based approach**, common information is captured once in a `component` assembly. Each instance of that component has its own `inventory-item` assembly, which cites the relevant component and only includes information unique to that instance.

For example, if the same Linux operating system is used as the platform for all database and web servers, most of the details about the Linux operating system can be captured once as a `component`. This includes information such as vendor name, version number, and patch level.

If four Linux instances are used, each instance is an `inventory item` with a unique IP address and MAC address. Only those unique pieces are captured at the inventory level. All four inventory-items point back to the `component` for vendor name, version number, and patch level.

Type: "software"
Name: "Database Product"
Vendor: "Vendor Name"
Version: "1.2.3"

Type: "software"
Name: "Web Server Product"
Vendor: "Vendor Name"
Version: "4.3.2"

Type: "software"
Name: "Operating System Product"
Vendor: "Vendor Name"
Version: "8.4.1"

Database Product
IPv4: 1.1.1.30
Operating System Product
IPv4: 1.1.1.30

Database Product
IPv4: 1.1.1.30
Operating System Product
IPv4: 2.1.1.30

Web Server Product
IPv4: 1.1.1.20
Operating System Product
IPv4: 1.1.1.20

Web Server Product

Operating System Product
IPv4: 2.1.1.20

Component-based Inventory Approach

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a s

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

FedRAMP Extensions & Allowed Values

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name="vendor-name"`
- `name="scan-type"`
  - **Valid:** `infrastructure, web, database`

	All Inventories			
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes
Software Example	123.45.78.400	123.45.78.400	No	No
Database Example	123.45.78.401	123.45.78.401	No	No

NIST Allowed Values

prop

- `name="virtual"`
  - **Valid:** yes, no
- `name="public"`
  - **Valid:** yes, no

prop

- `name="allows-authenticated-scan"`
  - **Valid:** yes, no
- `name="is-scanned"`
  - **Valid:** yes, no

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00	Yes	Base Config1	Cent				

FedRAMP Allowed Values

prop

- `name="asset-type"`
  - **Valid:** `os, database, web-server, dns-server, email-server, directory-server, pbx, firewall, router, switch, storage-array`

Other values are allowed for now.

Software and Database Inventories				Any Inventory				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

6.5.1. Flat File Approach

Flat-File Representation

```
<!-- cut -->
<system-implementation>
    <!-- interconnection -->
    <system-inventory>
        <inventory-item uuid="uuid-value" asset-id="unique-asset-id">
            <description><p>Flat-File Example (No implemented-c
            <prop name="ipv4-address" value="0.0.0.0"/>
            <prop name="ipv6-address" value="0000:0000:0000:000
            <prop name="virtual" value="no"/>
            <prop name="public" value="no"/>
            <prop name="fqdn" value="example.com"/>
            <prop name="uri" value="https://example/query?key=v
            <prop name="netbios-name" value="netbios-name"/>
            <prop name="mac-address" value="00:00:00:00:00:00"/
            <prop name="software-name" value="software-name"/>
            <prop name="version" value="V 0.0.0"/>
            <prop name="asset-type" value="os"/>
            <prop name="vendor-name" value="Vendor Name"/>
            <prop name="model" value="Model Number"/>
            <prop name="patch-level" value="Patch-Level"/>
            <prop name="serial-number" value="Serial #"/>
            <prop name="asset-tag" value="Asset Tag"/>
            <prop name="vlan-id" value="VLAN Identifier"/>
            <prop name="network-id" value="Network Identifier"/>
            <prop name="scan-type" ns="https://fedramp.gov/ns/oscal" value="infrastructure"/>
            <prop name="allows-authenticated-scan"  value="no">
                <remarks><p>If no, explain why. If yes, omit remarks field.</p></remarks>
            </prop>
            <prop name="baseline-configuration-name" value="Baseline Config. Name" />
            <prop name="physical-location" value="Physical location of Asset" />
            <prop name="is-scanned" value="yes"/>
            <prop name="function" value="Required brief, text-based description."/>
            <link rel="validation" href="#uuid-of-validation-component" />
            <status state="operational"/>
            <responsible-party role-id="asset-owner">
                <party-id>person-7</party-id>
            </responsible-party>
            <responsible-party role-id="asset-administrator">
                <party-id>it-dept</party-id>
            </responsible-party>
            <implemented-component component-uuid="component-uuid-value " />
            <remarks><p>COMMENTS: Additional information about this item.</p></remarks>
        </inventory-item>
        <!-- Repeat the inventory-item assembly for each item in the inventory -->
    </system-inventory>
    <!-- system-implementation remarks -->
</system-implementation>
```

NIST-Defined Identifier

Required Role ID may be one of the following:

- `asset-owner`
- `asset-administrator`
- `security-operations`
- `network-operations`
- `incident-response`
- `helpdesk`
- `configuration-management`
- `maintainer`
- `provider`

Other values are allowed.

XPath Queries

See Section 6.5.3, Inventory Data Locations and XPath Queries

NOTES:

The value of `asset-type` determines whether the identified asset-administrator is managing a system or an application. Currently, any FedRAMP-defined `asset-type` implies the management of a system, and therefore, is to be scanned as infrastructure.

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a s

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

FedRAMP Extensions & Allowed Values

prop (`ns="https://fedramp.gov/ns/oscal"`):

- `name=""vendor-name""`
- `name="scan-type"`
  - **Valid:** `infrastructure, web, database`

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00	Yes	Base Config1	Cent				

FedRAMP Allowed Values

prop

- `name="asset-type"`
  - **Valid:** `os, database, web-server, dns-server, email-server, directory-server, pbx, firewall, router, switch, storage-array`

Other values are allowed for now.

Software and Database Inventories				Any Inventory				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner

The `description` and `remarks` fields are *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit: https://pages.nist.gov/OSCAL/documentation/schema/model-concepts/datatypes/#markup-multiline

6.5.2. Component-based Approach

Component-based Representation

```
<!-- cut -->
<system-implementation>
    <component uuid="uuid-value" type="software">
        <prop name="virtual" value="no"/>
        <prop name="software-name" value="software-name"/>
        <prop name="version" value="V 0.0.0"/>
        <prop name="asset-type" value="operating-system"/>
        <prop name="vendor-name" value="Vendor Name"/>
        <prop name="model" value="Model Number"/>
        <prop name="patch-level" value="Patch-Level"/>
        <prop name="scan-type" ns="https://fedramp.gov/ns/oscal" value="infrastructure"/>
        <prop name="allows-authenticated-scan"  value="no">
            <remarks><p>If no, explain why. If yes, omit remarks field.</p></remarks>
        </prop>
        <prop name="baseline-configuration-name" value="Baseline Config. Name" />
        <prop name="function" value="Required brief, text-based description.">
            <remarks><p>Optional, longer, formatted description.</p></remarks>
        </prop>
        <link rel="validation" href="#uuid-of-validation-component" />
        <status state="operational"/>
        <responsible-party role-id="asset-owner">
            <party-id>person-7</party-id>
        </responsible-party>
        <responsible-party role-id="asset-administrator">
            <party-id>it-dept</party-id>
        </responsible-party>
    </component>
    <!-- service, interconnection -->
    <system-inventory>
        <inventory-item uuid="uuid-value" asset-id="unique-asse
            <description><p>If needed, describe this instance.<
            <prop name="ipv4-address" value="0.0.0.0"/>
            <prop name="public" value="no"/>
            <prop name="fqdn" value="example.com"/>
            <prop name="uri" value="https://example/query?key=v
            <prop name="mac-address" value=">00:00:00:00:00:00"
            <prop name="serial-number" value="Serial #"/>
            <prop name="vlan-id" value="VLAN Identifier"/>
            <prop name="network-id" value="Network Identifier"/>
            <prop name="is-scanned" value="yes" />
            <implemented-component component-uuid="component-uuid-value " />
            <remarks><p>COMMENTS: Additional information about this item.</p></remarks>
        </inventory-item>
        <!-- Repeat the inventory-item assembly for each use of the above component -->
    </system-inventory>
    <!-- system-implementation remarks -->
</system-implementation>
```

NIST-Defined Identifier

Required Role ID may be one of the following:

- `asset-owner`
- `asset-administrator`
- `security-operations`
- `network-operations`
- `incident-response`
- `helpdesk`
- `configuration-management`
- `maintainer`
- `provider`

Other values are allowed.

XPath Queries

See Section 6.5.3, Inventory Data Locations and XPath Queries

NOTES:

- If component-sample is an image of a Linux virtual machine (VM), and 10 instances of that VM are in use, there would be one (1) component assembly and ten (10) inventory-item assemblies, all referencing the same component.

6.5.3. Inventory Data Locations and XPath Queries

The following queries are intended to show where to find each piece of information within the system inventory template.

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES

All Inventories	**UNIQUE ASSET IDENTIFIER**	Unique Identifier associated with the asset. This Identifier should be used consistently across all documents, 3PAOs artifacts, and any vulnerability scanning tools. For OS/Infrastructure and Web Application Software, this is typically an IP address or URL/DNS name. For a database, it is typically an IP address, URL, or database name. A CSP's own naming scheme is also acceptable as long as it has unique identifiers.	Must be unique.	Mandatory for all inventory records.		**X**	**1**	`/*/system-implementation/system-inventory/inventory-item/prop[@asset-id="___"]/@value`
								
								OR
								
								`/*/system-implementation/component/prop[@name="asset-id"]/@value`
									The system-specific "Unique Asset Identifier" must be set as the asset-id flag on the inventory-item field.

	IPv4 or IPv6 Address	If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column.
		
		If a device has multiple IP addresses, then include one row in this inventory for each IP address.
				Optional, unless used as Identifier in vulnerability scans or security assessments.		**X**	**0 - ∞**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv4-address"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="ipv6-address"]/@value`
									One prop field per IP address, if more than one.

	Virtual	Is this asset virtual?	Yes or No.	Mandatory for OS/Infrastructure. Software, and Database.	X	**X**	**1**	`/*/system-implementation/component/prop[@name="virtual"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="virtual"]/@value`
									Must have "Virtual" at the inventory item-level either explicitly, or via a linked component.
									
									May define it at component level and propagate to inventory-item.

	Public	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	Yes or No.	Mandatory for OS/Infrastructure. Software, and Database.		**X**	**1**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="public"]/@value`	

	DNS Name or URL	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.	Valid DNS name or URL.	Optional, unless used as Identifier in vulnerability scans or security assessments.		**X**	**0 - ∞**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="fqdn"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="uri"]/@value`
									May use either DNS name, URL or both. Use a separate prop field for each DNS name and/or URL.

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
OS/Infrastructure Inventory	**NetBIOS Name**	If available, state the NetBIOS name. May be left blank if one does not exist, or dynamic.	Valid NetBIOS name.	Optional, unless used as Identifier in scans or security assessments.		**X**	**0 - ∞**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="netbios-name"]/@value`	One prop field per NetBIOS name, if more than one.
	MAC Address	If available, state the MAC Address. May be left blank if one does not exist, or dynamic.	Valid MAC Address.	Optional, unless used as Identifier in scans or security assessments.		**X**	**0 - ∞**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="mac-address"]/@value`	One prop field per MAC address, if more than one.

	Authenticated Scan	Is the asset is planned for an authenticated scan?	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	**X**	**1**	`/*/system-implementation/component/prop[@name="allows-authenticated-scan"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="allows-authenticated-scan"]/@value`
									Must have "Authenticated-Scan" at the inventory-item level either explicitly or via a linked component.
									
									May define it at component level and propagate to inventory-item.

	Baseline Configuration Name	If available, provide the name of the configuration template used within the CSP configuration management.	.	Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="baseline-configuration-name"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="baseline-configuration-name"]/@value`
									Must have "Baseline Configuration Name" at the inventory-item level either explicitly or via a linked component.
									
									May define it at component level and propagate to inventory-item.

	OS Name and Version	Operating System Name and Version running on the asset.		Optional for OS/Infrastructure. Leave blank for Software and Database.		**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								
								`/*/system-implementation/component/prop[@name="version"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]/@value`
									Use software name and version, and set asset-type of "os".
									Required for operating systems.
									
									Must have "OS Name and Version" at the inventory-item level either explicitly or via a linked component. May define it at the component level and propagate to inventory item.

	Location	Physical location of hardware. Could include Data Center ID, Cage#, Rack# or other meaningful location identifiers.	Valid locations for CSP infrastructure.	Optional for OS/Infrastructure. Leave blank for Software and Database.		**X**	**0 or 1**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="physical-location"]/@value`	

	Asset Type	Simple description of the asset's function (e.g., Router, Storage Array, DNS Server, etc.)		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	**X**	**1**	`/*/system-implementation/component/prop[@name="asset-type"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item[@name="asset-type"]/@value`
									Must use an Accepted Value (see Registry) if an applicable one exists.
									
									Must have "Asset Type" at the inventory-item level, either explicitly or via a linked component. May define it at component level and propagate to inventory-item.

	Hardware Make/Model	Name of the hardware product and model.		Mandatory for OS/Infrastructure. Leave blank for Software and Database.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="vendor-name"]/@value`
								
								`/*/system-implementation/component/prop[@name="model"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="hardware-model"]/@value`
									Must have "Hardware Vendor" and "Hardware Model" at the inventory item-level either explicitly, or via a linked component. May define it at component level and propagate to inventory-item.
									
									NOTE: @name="model" at component level, but @name="hardware-model" at inventory level.

	In Latest Scan	Should the asset appear in the network scans and can it be probed by the scans	Yes or No.	Mandatory for OS/Infrastructure. Leave blank for Software and		**X**	**1**	`/*/system-implementation/system-inventory/inventory-item/prop[@name="is-scanned"]/@value`	

		Guidance	Valid Values	Requirement	Component	Inventory-Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES

Software and Database Inventories	**Software/ Database Vendor**	Name of Software or Database vendor.	If open source (e.g., there is no "vendor), enter "Open Source" as the vendor name.	Mandatory for Software and Database. Leave blank for OS/Infrastructure.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="vendor-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
									Must have "Software/Database Vendor" at the inventory-item level either explicitly, or via a linked component.
									
									May define it at component level and propagate to inventory-item.

	Software/ Database Name & Version	Name of Software or Database product and version number.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="software-name"][@ns="https://fedramp.gov/ns/oscal"]/@value`
								
								`/*/system-implementation/component/prop[@name="version"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-name"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-version"]/@value`
									Required for software or database. Omit for OS/Infrastructure

	Patch Level	If applicable.		Optional if applicable. Otherwise, leave blank.	**X**	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="patch-level"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="software-patch-level"]/@value`
									The "Patch Level" may be specified at the component or inventory-item level.

	Function	For Software or Database, the function provided by the Software or Database for the system.		Mandatory for Software or Database. Leave blank for OS/Infrastructure.	X	**X**	**0 or 1**	`/*/system-implementation/component/prop[@name="function"]/@value`
								
								`/*/system-implementation/component/prop[@name="function"]/remarks`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="function"]/@value`
								
								`/*/system-implementation/system-inventory/inventory-item/prop[@name="function"]/remarks`
									Must have a brief, text-base "function" description in the value flag at the inventory item-level.
									
									May define it at component level and propagate to inventory-item.
									
									May have a separate "function" at the component level.
									
									May have an expanded, formatted function description in the remarks.

.

		Guidance	Valid Values	Requirement	Component	Inventory -Item	OSCAL Cardinality	Data Location: XPath Notation (CASE SENSITIVE)	NOTES
Any Inventory	**Comments**	Any additional information that could be useful to the reviewer.		Optional for OS/Infrastructure, Software and Database.	X	X	**0 or 1**	/*/system-implementation/component/remarks /*/system-implementation/system-inventory/inventory-item/remarks	May have comments in either the component level, inventory-item level or both.
	Serial #/Asset Tag#	Product serial number or internal asset tag #.		Optional for OS/Infrastructure, Software, and Database.		**X**	**0 or 1**	/*/system-implementation/system-inventory/inventory-item/prop[@name="serial-number"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="asset-tag"]/@value	
	VLAN/ Network ID	Virtual LAN or Network ID.		Optional for OS/Infrastructure, Software, and Database.		**X**	**0 - ∞**	/*/system-implementation/system-inventory/inventory-item/prop[@name="vlan-id"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="network-id"]/@value	
	System Administrator/ Owner	Name of the system administrator or owner.		Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	X	**X**	**0 - ∞**	COMPONENT OWNER (Person): /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-uuid]/name COMPONENT ADMINISTRATOR (Org): /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-uuid]/name INVENTORY ITEM OWNER (Person): /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-uuid]/name INVENTORY ITEM ADMINISTRATOR (Org): /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-uuid]/name	Must have "System Owner/Administrator" at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "system owner/administrator" at the component level.
	Application Administrator/ Owner	Name of the application administrator or owner.		Optional for OS/Infrastructure, Software, and Database.	X	**X**	**0 - ∞**	COMPONENT OWNER: /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-owner"]/party-uuid]/name CMPONENT ADMINISTRATOR: /*/metadata/party[@uuid=/*/system-implementation/component/responsible-role[@role-id="asset-administrator"]/party-uuid]/name INVENTORY ITEM OWNER: /*/metadata/party[@id=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-owner"]/party-id]/person/person-name INVENTORY ITEM ADMINISTRATOR: /*/metadata/party[@uuid=/*/system-implementation/system-inventory/inventory-item/responsible-party[@role-id="asset-administrator"]/party-uuid]/name	Must have "Application Owner/Administrator" at the inventory item-level. May define it at component level and propagate to inventory-item. May have a separate "system owner/administrator" at the component level.
ADDITIONAL	**Scan Type**	Indicate which scan type(s) the item is subjected to.	infrastructure, database, web-server	Mandatory	X	**X**	**1 - ∞**	/*/system-implementation/component/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="scan-type"][@ns="https://fedramp.gov/ns/oscal"]/@value	Valid values: infrastructure, web, database. If more than one type is applicable, use one field per type.
	FIPS 140-2 Validation	Indicate the certificate information for an inventory item with a FIPS 140-2 validated cryptographic module.	component-id	Mandatory for any item involving cryptography. Omit otherwise.	X	**X**	**1w - ∞**	/*/system-implementation/component/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]/@value /*/system-implementation/system-inventory/inventory-item/prop[@name="validation"][@ns="https://fedramp.gov/ns/oscal"]/@value	If an item has more than one cryptographic module, use one entry per validation certificate. May define "FIPS 140-2 validation" at the component level and propagate to the inventory-item level.

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

	All Inventories				
	UNIQUE ASSET IDENTIFIER	IPv4 or IPv6 Address	Virtual	Public	DNS Name or URL
OS/Infrastructure Example	123.45.78.90	123.45.78.90	No	Yes	linux01.iaas.org
Software Example	123.45.78.400	123.45.78.400	No	No	
Database Example	123.45.78.401	123.45.78.401	No	No	

OS/Infrastructure Inventory								
NetBIOS Name	MAC Address	Authenticated Scan	Baseline Configuration Name	OS Name and Version	Location	Asset Type	Hardware Make/Model	In Latest Scan
linux01	00:00:00:00:00:00	Yes	Base Config1	CentOS 5.1	n/a	Web Server	Acme Server	No

Software and Database Inventories				Any Inventory				
Software/ Database Vendor	Software/ Database Name & Version	Patch Level	Function	Comments	Serial #/Asset Tag#	VLAN/ Network ID	System Administrator/ Owner	Application Administrator/ Owner
Acme Software	Acme CloudApp v1.0		CRM					
Oracle	Oracle v11		Records Management					

XPath Queries

```
Number of Inventory Items:
  count(/*/system-implementation/system-inventory/inventory-item)

Number of Hardware Components:
  count(/*/system-implementation/component[@type="hardware"])

Number of Software Components:
  count(/*/system-implementation/component[@type="software"])

In Latest Scan?:
  /*/system-implementation/system-inventory/inventory-item[1]/prop[@name="is-
  scanned"]/@value

List Inventory Items Not Scanned:
  /*/system-implementation/system-inventory/inventory-item/prop[@name="is-
  scanned"][@value='no']/../prop[@name='ipv4-address']

List of Reasons Inventory Items Were Not Scanned:
  /*/system-implementation/system-inventory/inventory-item/prop[@name="is-
  scanned"][@value='no']/remarks/node()
```

Replace "[1]" with "[2]", "[3]", etc.

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/reference/datatypes/

ATTACHMENT 13 FEDRAMP INVENTORY WORKBOOK

All Authorization Packages must the Inventory attachment, which will be reviewed for quality.

When completed, FedRAMP will accept this inventory workbook as the inventory information required by the following:

- System Security Plan
- Security Assessment Plan
- Security Assessment Report
- Information System Contingency Plan
- Initial POAM
- Monthly Continuous Monitoring (POAM or as a separate document)

The FedRAMP Inventory Workbook can be found on the following FedRAMP website page: Templates.

Note: A complete and detailed list of the system hardware and software inventory is required per NIST SP 800-53, Rev 4 CM-8.

All Inventories			
IPv4 or IPv6 Address	**Virtual**	**Public**	**DNS Name or URL**
If available, state the IPv4 or IPv6 address of the inventory item. This can be left blank if one does not exist, or if it is a dynamic field. If the IP address is used as the Unique Asset Identifier, then this field will duplicate the contents of the Unique Asset Identifier column. If a device has multiple IP addresses, then include one row in this inventory for each IP address.	Is this asset virtual?	Is this asset a public facing device? That is, is it outside the boundary? If so, it is an entry point.	If available, state the DNS name or URL of the inventory item. This can be left blank if one does not exist, or it is a dynamic field.
	Yes or No.	Yes or No.	Valid DNS name or URL.
Optional, unless used as Identifier in vulnerability scans or security assessments.	Mandatory for OS/Infrastructure, Software, and Database.	Mandatory for OS/Infrastructure, Software, and Database.	Optional, unless used as Identifier in vulnerability scans or security assessments.

Any Inventory				
Comments	**Serial #/Asset Tag#**	**VLAN/ Network ID**	**System Administrator/ Owner**	**Application Administrator/ Owner**
Any additional information that could be useful to the reviewer.	Product serial number or internal asset tag #.	Virtual LAN or Network ID.	Name of the system administrator or owner.	Name of the application administrator or owner.
Optional for OS/Infrastructure, Software and Database.	Optional for OS/Infrastructure, Software, and Database.	Optional for OS/Infrastructure, Software, and Database.	Mandatory for HIGH impact systems. Optional for Low and Moderate impact systems.	Optional for OS/Infrastructure, Software, and Database.

Unlike most XPath 2.0 queries in this document, the following queries cannot be easily converted to XPath 1.0. If working with XPath 1.0, it may be necessary to perform each search with two separate queries. These queries will list all the IPv4 addresses for each scan type (infrastructure, web, and database), whether using the flat-file inventory approach or the component-based approach.

XPath 2.0 Queries

```
IPv4 Address of All Inventory Items Identified for Infrastructure Scanning:
  distinct-values( (let $key:=/*/system-implementation/component[prop [@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='infrastructure']/@uuid return /*/system-
  implementation/system-inventory/inventory-item [implemented-component/@component-
  uuid=$key]/ prop[@name='ipv4-address']) | (/*/system-implementation/system-
  inventory/inventory-item/prop[@name='ipv4-address'][../prop[@name='scan-
  type'][@ns='https://fedramp.gov/ns/oscal']  [string(.)='infrastructure']]) )

IPv4 Address of All Inventory Items Identified for Web Scanning:
  distinct-values( (let $key:=/*/system-implementation/component[prop[@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='web']/@uuid return /*/system-implementation/system-
  inventory/inventory-item [implemented-component/@component-uuid=$key]/prop[@name='ipv4-
  address']) | (/*/system-implementation/system-inventory/inventory-item/prop[@name='ipv4-
  address'][../prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal'][string(.)='web']]))

IPv4 Address of All Inventory Items Identified for Database Scanning:
  distinct-values( (let $key:=/*/system-implementation/component[prop [@name='scan-type']
  [@ns='https://fedramp.gov/ns/oscal']='database']/@uuid return /*/system-implementation/
  system-inventory/inventory-item [implemented-component/@component-uuid=$key]/
  prop[@name='ipv4-address']) | (/*/system-implementation/system-inventory/inventory-item/
  prop[@name='ipv4-address'][../prop[@name='scan-type'][@ns='https://fedramp.gov/ns/oscal']
  [string(.)='database']]))

IPv4 Address of All Items Where an Authenticated Scan is Possible:
  distinct-values( (/*/system-implementation/system-inventory/inventory-item/prop
  [@name='ipv4-address'][../prop[@name="allows-authenticated-scan"][@value='yes']] ) | (let
  $key:=/*/system-implementation/component[prop [@name='allows-authenticated-
  scan'][@value='yes']]/@uuid return /*/system-implementation/system-inventory/inventory-item
  [implemented-component/@component-uuid=$key]/prop[@name='ipv4-address']))

IPv4 Address of All Items Where an Authenticated Scan is Not Possible:
  distinct-values( (/*/system-implementation/system-inventory/inventory-item/
  prop[@name='ipv4-address'][../prop[@name="allows-authenticated-scan"][@value='no']] ) | (
  let $key:=/*/system-implementation/component[prop [@name='allows-authenticated-
  scan'][@value='no']]/@uuid return /*/system-implementation/system-inventory/inventory-item
  [implemented-component/@component-uuid=$key]/prop[@name='ipv4-address']) )

Authenticated Scan Justification (if Authenticate Scan is "no"):
  /*/system-implementation/system-inventory/inventory-item/prop[@name="allows-
  authenticated-scan"][@value="no"]/remarks/node()

OR
  /*/system-implementation/component/prop[@name="allows-authenticated-scan"]
  [@value="no"]/remarks/node()
```

The `remarks` field is *Markup multiline*, which enables the text to be formatted. This requires special handling. See *Section 2.6 Handling OSCAL Data Types* in the *Guide to OSCAL-based FedRAMP Content*, or visit:
https://pages.nist.gov/OSCAL/reference/datatypes/

7. GENERATED CONTENT

The following artifacts are historically generated by hand to summarize content found in other portions of the FedRAMP SSP. When using OSCAL, these artifacts can be generated from content found elsewhere in this document. This includes the:

- **Control Information Summary (CIS)**
- **Customer Responsibility Matrix (CRM)**

If delivering SSP content in OSCAL, CSPs are no longer required to manually generate and maintain these artifacts, provided the content in their OSCAL-based FedRAMP SSP remains accurate.

Tool developers are encouraged to develop their own solutions to generating this content.

7.1. Generating the Control Information Summary (CIS)

There are many ways a tool developer can generate the CIS. FedRAMP is developing an Extensible Stylesheet Language Transformation (XSLT) file to generate the FedRAMP CIS. When ready, FedRAMP will make this freely available to the public here:

https://github.com/GSA/fedramp-automation/tree/master/dist/content/resources

7.2. Generating the Customer Responsibility Matrix (CRM)

There are many ways a tool developer can generate the CRM. FedRAMP is developing an XSLT file to generate the FedRAMP CRM. When ready, FedRAMP will make this freely available to the public here:

https://github.com/GSA/fedramp-automation/tree/master/dist/content/resources

Useful CRM XPath Queries

```
Flat-File CRM Query:
  //control-implementation/implemented-requirement/prop[@name="control-
  origination"][@ns="https://fedramp.gov/ns/oscal"][@value="customer-
  configured" or @value="customer-provided"]/remarks/node()

Component-based CRM Query:
  //control-implementation/implemented-requirement/statement/by-component
  [@component-id="customer"]/description
```

APPENDIX A. WORKING WITH COMPONENTS

NIST designed OSCAL such that a system architect can express all aspects of the system as components. A component is anything that can satisfy a control requirement. This includes hardware, software, services, and underlying service providers, as well as policies, plans, and procedures. There are several ways to use components in an OSCAL-based SSP. The following defines FedRAMP's minimum initial use.

Anything that can satisfy a control requirement is a component, including hardware, software, services, policies, plans, and procedures.

This section will likely be updated as NIST continues to evolve its approach to components in OSCAL, and as FedRAMP receives feedback from stakeholders.

FedRAMP-defined component identifiers are cited in relevant portions of this document and summarized in the FedRAMP OSCAL Registry.

Minimum Required Components

There must be a component that represents the entire system itself. It should be the only component with the `component-type` set to "`system`".

The following is an example of defined components.

Minimum Required Component Representation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->

    <!-- This System -->
    <component uuid="uuid-value" type="this-system" >
        <title>This System</title>
        <description><p>
            The entire system as depicted in the system authorization boundary.
        </p></description>
        <status state="operational" />
    </component>

</system-implementation>
```

NIST has clarified the approach to leveraged authorizations and the CRM. Leveraged authorizations and customer responsibility content are no longer handled as components. These scenarios require special handling as described in Section 5, Security Controls.

Common Additional Components

For each FIPS 140 validated module, there must be a component that represents the validation certificate itself. For more information about this, see the *FIPS 140 Validated Components* Section.

Common Additional Component Representation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->
    <!-- System Copmponent -->

    <!-- Ports, Protocols and Services Entry -->
    <component uuid="uuid-of-service" type="service">
        <title>[SAMPLE]Service Name</title>
        <description><p>Describe the service</p></description>
        <purpose>Describe the purpose the service is needed.</purpose>
        <prop name="used-by" value="What uses this service?"/>
        <status state="operational" />
        <protocol name="http">
            <port-range start="80" end="80" transport="TCP"/>
        </protocol>
        <protocol name="https">
            <port-range start="443" end="443" transport="TCP"/>
        </protocol>
    </component>

    <!-- FIPS 140 Validation Certificate Information -->
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="validation">
        <title>Module Name</title>
        <description><p>FIPS 140 Validated Module</p></description>
        <prop name="validation-type" value="fips-140-2"/>
            <prop name="validation-reference" value="0000"/>
            <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" />
            <status state="operational" />
    </component>

    <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

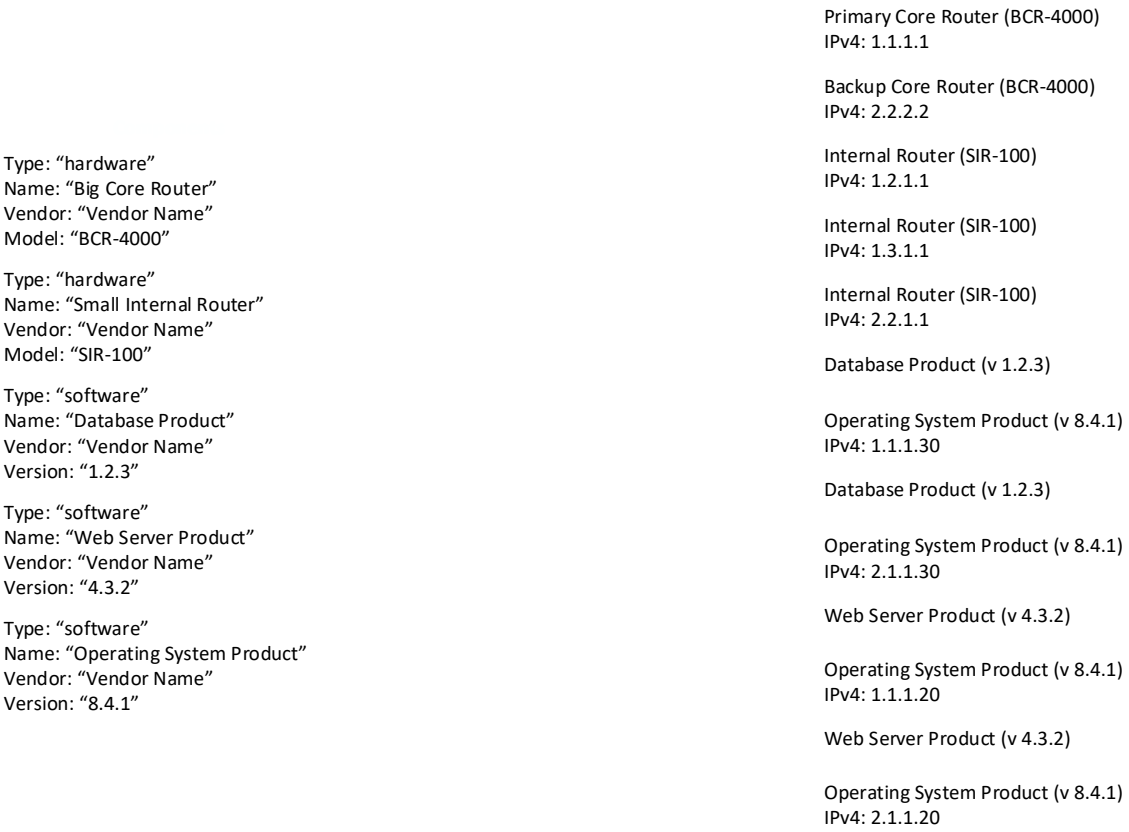
NIST has clarified the approach to leveraged authorizations and the CRM. Leveraged authorizations and customer responsibility content are no longer handled as components. These scenarios require special handling as described in Section 5, Security Controls.
The component-type "service" is now used for information typically found in the Ports, Protocols, and Services table, as described in Section 4.25, Ports, Protocols and Services.

Components as a Basis for System Inventory

NIST's approach to component-based system modeling is to reduce redundancy of information and increase flexibility. NIST accomplishes this with separate component and inventory item modeling.

This is a one-to-many relationship. One component to many inventory item instances.

For example, if an open source operating system (OS) is used in many places throughout the system, it is defined once as a component. All information about the product, vendor, and support are modeled within the component detail. If the OS is used four times within the system, each use is an inventory item, with details about that specific information, such as IP address.



Relationship of Components and Inventory Items

FedRAMP requires a component assembly for each model of infrastructure device used, and each version of software and database used within the system. FedRAMP is not asking for more detail than provided in the legacy inventory workbook. Only that the information is organized differently.

As NIST continues to evolve its component approach, FedRAMP will re-evaluate its approach to system inventory representation.

FIPS 140 Validated Components

NIST's component model treats independent validation of products and services as if that validation were a separate component. This means when using components with FIPS 140 validated cryptographic modules, there must be two `component` assemblies:

- **The Validation Definition**: A component definition that provides details about the validation.
- **The Product Definition**: A component definition that describes the hardware or software product.

The validation definition is a component definition that provides details about the independent validation. It's type must have a value of "validation". In the case of FIPS 140 validation, this must include a `link` field with a `rel` value set to "validation-details". This link must point to the cryptographic module's entry in the NIST Computer Security Resource Center (CSRC) Cryptographic Module Validation Program Database.

The product definition is a product with a cryptographic module. It must contain all of the typical component information suitable for reference by inventory-items and control statements. It must also include a `link` field with a `rel` value set to "validation" and an `href` value containing a URI fragment. The Fragment must start with a hashtag (#) and include the UUID value of the validation component. This links the two together.

Component Representation: Example Product with FIPS 140-2 Validation

```
<!-- system-characteristics -->
<system-implementation>
    <!-- user -->
    <!-- Minimum Required Components -->

    <!-- FIPS 140-2 Validation Certificate Information -->
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="validation">
        <title>Module Name</title>
        <description><p>FIPS 140-2 Validated Module</p></description>
        <prop name="validation-type" value="fips-140-2"/>
            <prop name="validation-reference" value="0000"/>
            <link href="https://csrc.nist.gov/projects/cryptographic-module-
validation-program/Certificate/0000" rel="validation-details" />
            <status state="operational" />
    </component>

    <!-- FIPS 140-2 Validated Product -->
    <component uuid="uuid-value" type="software" >
        <title>Product Name</title>
        <description><p>A product with a cryptographic module.</p></description>
        <link href="#uuid-of-validation-component" rel="validation" />
        <status state="operational" />
    </component>

    <!-- service -->
</system-implementation>
<!-- control-implementation -->
```

APPENDIX B. CONVERTING A LEGACY SSP TO OSCAL

NIST designed OSCAL such that a system architect can express all aspects of the system as components. A component is anything that can satisfy a control requirement. This includes hardware, software, services, and underlying service providers, as well as policies, plans, and procedures.

Anything that can satisfy a control requirement is a component, including hardware, software, services, policies, plans, and procedures.

OSCAL is also designed to support legacy conversion of SSPs without individual components defined, and enables an SSP author to migrate to the component approach gradually over time. In this instance, only a single component is initially required, representing the system as a whole and designated with the special component type, "`this-system`". The following provides an example of FedRAMP's minimum required component approach:

Example control for legacy SSP conversion

```
<!-- system-characteristics -->
<system-implementation>
    <!-- Include a separate component for each relevant certificate -->
    <component uuid="uuid-value" type="this-system">
        <title>System Name</title>
        <description>
            <p>Component representing the entire system.</p>
        </description>
    </component>
</system-implementation>
<control-implementation>
    <description><p>FedRAMP SSP Template Section 13</p></description>
    <implemented-requirement control-id="ac-1" uuid="uuid-value">
        <statement statement-id="ac-1_stmt.a" uuid="uuid-value">
            <by-component component-uuid="Component-uuid-value" uuid="uuid-
value">
                <description>
                    <p>Describe how Part a is satisfied within the system.</p>
                </description>
            </by-component>
        </statement>
        <statement statement-id="ac-1_stmt.b.1" uuid="uuid-value">
            <by-component component-uuid="Component-uuid-value" uuid="uuid-
value">
                <description>
                    <p>Describe how Part b 1 is satisfied within the system.</p>
                </description>
            </by-component>
        </statement>
        <statement statement-id="ac-1_stmt.b.2" uuid="uuid-value">
            <by-component component-uuid="Component-uuid-value" uuid="uuid-
value">
                <description>
                    <p>Describe how Part b 2 is satisfied within the system.</p>
                </description>
            </by-component>
        </statement>
    </implemented-requirement>
</control-implementation>
```